Divisores primos del orden de productos de elementos en grupos finitos

Azahara Sáez Porras

dirigida por

Alexander Moretó Quintana

Facultat de Ciències Matemàtiques

Programa de Doctorat en Matemàtiques

Burjassot, Setembre, 2018

A mis padres y mi hermana

Índice general

Declaro que esta disertación titulada *Divisores primos del orden de productos de elementos en grupos finitos* y el trabajo presentado en ella son míos. Lo confirmo:

- Este trabajo se realizó total o principalmente mientras se cursaban los estudios para la obtención del título de Doctor en la Universitat de València.
- Cuando se han consultado las publicaciones de otras personas, siempre se ha indicado claramente.
- Donde se han citado los trabajos de otras personas, siempre se ha dado la fuente de tales publicaciones. Con la excepción de tales citas, esta disertación es completamente trabajo propio.
- Han sido reconocidas todas las fuentes de ayuda.

Burjassot, 13 de septiembre de 2018

Azahara Sáez Porras

Declaro que esta disertación presentada por **Azahara Sáez Porras** titulada *Divisores primos del orden de productos de elementos en grupos finitos* se ha realizado bajo mi supervisión en la Universitat de València. También indico que este trabajo corresponde al proyecto de tesis aprobado por esta institución y cumple todos los requisitos para obtener el título de Doctor en Matemáticas.

Burjassot, 13 de septiembre de 2018

Alexander Moretó Quintana

Agradecimientos

En primer lugar, quisiera dar las gracias a Alex, quien confió en mí y aceptó dirigirme esta tesis; gracias por guiarme en el camino y ayudarme para que esta memoria fuera una realidad. Gracias Antonio, porque la estancia en el IMAC fue un gran paso hacia delante y un enorme aprendizaje. Gracias por tanto en tan poco tiempo. Gracias también a Gabriel, mi tutor y mi conciencia, por apoyarme y confiar en mí. Además, quisiera extender toda mi gratitud al comité evaluador de la tesis por todas las aportaciones y comentarios recibidos.

Por aguantarme todos estos años y por hacer todo lo posible para que pudiera seguir estudiando, gracias papá y mamá porque sin vosotros esto no sería posible. Gracias por confiar en mí y darme el aliento que tantas veces he necesitado, desde el primer día que puse el pie en esta facultad. Gracias también a ti tata, por estar ahí siempre, porque nos basta una mirada para entendernos. Gracias por darme a Andrea, que con sus sonrisas y sus "te quiero tía" también ha contribuido en el desarrollo de esta tesis. A mi yaya, por nuestras noches de pizzas y películas; por poder verme acabar este proyecto. Gracias a ti cielo, llevamos juntos el mismo tiempo que llevo con el doctorado, nadie mejor que tú sabe de mis noches en vela y mis nervios, mis disgustos y mis alegrías. Gracias por intentar siempre animarme y hacerme reír. También quiero agradecer a mis amigas, Sus y Nuri, porque las tres juntas podemos con todo. A Anita y Vega por nuestras cenas y nuestras risas. En general, a todas las personas que me han acompañado estos cuatro años, a los que no están pero que seguirán jaleándome desde el cielo y a los que espero que sigan muchos años más con nosotros.

Por último, quiero agradecer a todo el departamento el trato recibido desde el inicio de esta tesis. En especial, gracias a Lucía Sanus por ser nuestra amiga y nuestra biblia. No me puedo olvidar de mis compañeros doctorandos, incluyendo a Lydia y muy especialmente a mi compañera de despacho Noelia Rizo, gracias a todos por tantas confidencias, ayuda y buenos ratos.

Esta memoria ha sido redactada en el Departament de Matemàtiques de la Universitat de València durante el periodo de disfrute de un Contrato Predoctoral (ayuda BES-2014-068325) dentro del Programa Estatal de Promoción del Talento y su Empleabilidad del Plan Estatal de Investigación Científica y Técnica y de Innovación 2013–2016 Orden ECC/1402/2013 Ministerio de Economía y Competitividad.

Esta investigación ha sido parcialmente financiada por los proyectos: "Representaciones y caracteres de grupos finitos, II – MTM2013-40464-P" y "Representaciones y caracteres de grupos finitos, III – MTM2016-76196-P".

Introducción

Todos los grupos que consideramos en este trabajo son finitos. Esta memoria está dividida en cinco capítulos, más tres apéndices. Todos los resultados que se encuentran aquí son originales, salvo las demostraciones del Teorema 2.5 y el Teorema 2.14. Denotamos por Teorema A, B, C… a los teoremas principales de esta tesis que podemos encontrar en [**3**], [**4**] y [**33**]. Además, el trabajo realizado durante el doctorado ha dado lugar a otros problemas abiertos que aparecen como Cuestión $1, 2, 3\dots$ y pueden ser objeto de más investigación en el futuro.

Un tema clásico en Teoría de Grupos es el estudio de la relación entre la estructura de un grupo finito y sus longitudes de clases de conjugación o sus grados de caracteres. Originalmente, el objetivo de esta tesis era la obtención de resultados sobre órdenes de elementos análogos a los ya existentes para clases de conjugación o caracteres. Finalmente, hemos obtenido resultados novedosos sobre órdenes de elementos que no existían en la literatura para grados de caracteres o longitudes de clases de conjugación.

En esta memoria estudiamos qué información puede obtenerse sobre la estructura de un grupo a partir de la relación existente entre los órdenes de ciertos elementos y de sus productos. Uno de los principales resultados de este tipo es la caracterización de J. G. Thompson de los grupos resolubles. En [**40**], como consecuencia de la clasificación de los grupos simples minimales, Thompson demuestra que un grupo G es resoluble si y solo si no existen elementos no triviales $x, y, z \in G$ de órdenes coprimos dos a dos tales que $xyz = 1$. En 2015, R. M. Guralnick y P. H. Tiep [**18**] probaron que basta suponer la no existencia de tales elementos de orden potencia de primo para garantizar la resolubilidad. Motivados por este resultado, uno de los objetivos de esta tesis es obtener la versión para elementos de orden potencia de primo del Teorema de B. Baumslag y J. Wiegold [**5**], el cual afirma que un grupo G es nilpotente si y solo si para todo par de elementos $x, y \in G$ de orden coprimo, se tiene que $o(xy) = o(x)o(y)$, donde $o(x)$ denota el orden del elemento x. A raíz de la obtención de esta versión (Corolario B, Capítulo 3), obtenemos otras similares, además de una serie de resultados locales, que detallamos a continuación.

En el Capítulo 1 establecemos la notación y recordamos algunos resultados y definiciones generales de Teoría de Grupos que nos serán de utilidad.

En el Capítulo 2 mencionamos resultados ya conocidos que involucran órdenes de elementos y en los que se obtiene información sobre la estructura del grupo o se da un criterio de pertenencia de un elemento dado a un subgrupo normal relevante. Además, obtenemos variantes del Teorema de Thompson. Las demostraciones de algunas de estas variantes se alejan un poco de la naturaleza del resto de resultados de esta tesis, por ello, dichas pruebas se pueden encontrar en el Apéndice A. Por último, damos la prueba original del Teorema de Baumslag y Wiegold y comentamos las primeras ideas que surgen a partir de dicho teorema.

En el Capítulo 3 empezamos obteniendo una caracterización de los grupos nilpotentes al estilo de la de Guralnick y Tiep para grupos resolubles. Más precisamente, demostramos que un grupo G es nilpotente si y solo si para todos los elementos $x, y \in G$ de órdenes coprimos y de orden potencia de primo, el conjunto de primos que divide a $o(x)o(y)$ está contenido en el conjunto de primos que divide a $o(xy)$ (Teorema A). Después, nos centramos en obtener versiones locales de dicho teorema. Por un lado, probamos que un grupo G tiene π-subgrupos de Hall nilpotentes si se cumple que para todos los π-elementos $x, y \in G$ de órdenes coprimos y de orden potencia de primo, el conjunto de primos que divide a $o(x)o(y)$ está contenido en el conjunto de primos que divide a $o(xy)$, donde π es un conjunto de primos que divide al orden del grupo G (Teorema C). Este resultado se convierte en un "si y solo si" cuando el grupo es π-separable (Teorema D). Por otro lado, obtenemos la caracterización de la existencia de subgrupos de Hall normales, en particular, caracterizaciones de los grupos p-cerrados y p-nilpotentes. Por ejemplo, demostramos que dado un primo p, un grupo G tiene un p-subgrupo de Sylow normal si y solo si para todo primo $q \neq p$, q divide a $o(xy)$ para todo p-elemento x y para todo q-elemento y. Los resultados principales de este capítulo aparecen en [**4**] y [**33**]. Además, recogemos una serie de cuestiones y resultados relacionados con los anteriores. Una de estas cuestiones ha dado lugar a estudiar problemas sobre bases de Sylow y números de Sylow. Estos resultados se encuentran en el Apéndice C.

En el Capítulo 4 pretendemos obtener resultados en la línea de los del Capítulo 3 pero para caracterizar la pertenencia de un elemento fijo a ciertos subgrupos relevantes. Uno de los problemas principales que consideramos en este capítulo es si es cierto que un p-elemento $x \in G$ cumple que $x \in \mathbf{O}_p(G)$ si y solo si para todo primo $q \neq p$, q divide a $o(xy)$ para todo q-elemento no trivial y. Hemos demostrado que esta pregunta tiene una respuesta afirmativa para todos los grupos que no contengan factores de composición simples de tipo Lie en característica p y que un contraejemplo minimal a dicha pregunta es un grupo almost-simple con socle uno de estos grupos. En esta memoria, debido a su complejidad, no incluiremos la demostración en el caso de grupos almost-simple con socle de tipo Lie en característica coprima con p. Sin embargo, algunas de las técnicas utilizadas son similares a las que se muestran en el Apéndice A, donde puede encontrarse también la prueba en los casos que el socle sea un grupo simple esporádico o alternado. La prueba completa puede encontrarse en [**3**].

Por último, en el Capítulo 5 demostramos algunos resultados que hemos obtenido análogos a los vistos en los capítulos centrales pero para clases de conjugación y caracteres. El objetivo es tratar de caracterizar los grupos G que cumplen que para todo par de elementos $x, y \in G$ de órdenes coprimos se tiene que $x^G y^G = (xy)^G$, donde x^G denota la clase de conjugación del elemento x. Hemos conseguido probar que estos grupos son resolubles y clasificar una familia de ellos, pero dada la abundancia de tales grupos parece complicado obtener una clasificación completa. Al final del capítulo veremos un resultado que sí caracteriza los grupos nilpotentes como en el Teorema de Baumslag y Wiegold pero con longitudes de clases de conjugación.

Capítulo 1

Preliminares

La finalidad principal de este capítulo es fijar la notación que utilizaremos a lo largo de la memoria, así como recordar conceptos y resultados que nos serán de utilidad. La mayoría de los resultados y notación de la que hacemos uso pueden encontrarse en la literatura clásica de Teoría de Grupos. Véase, por ejemplo, los libros [**23**], [**24**] y [**38**].

Dado un entero n, denotamos por $\pi(n)$ al conjunto de primos que dividen a n. Sea π un conjunto de primos. Decimos que n es un π-número si todos los primos divisores de n pertenecen a π. Dado un entero n, si $n = p^a b$, con $(p, b) = 1$, diremos que p^a es la p-parte de n. Esta noción se puede extender a un conjunto de primos $\pi = \{p_1, \ldots, p_r\}$. Si $n = ab = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} b$ y $(a, b) = 1$, entonces a es la π-parte de n. Por otra parte, se tiene que π' es el conjunto de todos los números primos que no están en π.

Recordamos que todos los grupos son finitos. Dado un grupo G, denotamos por $o(x)$ al orden del elemento $x \in G$ y por $\pi(G)$ al conjunto $\pi(|G|)$. Dado G un grupo y $g \in G$, podemos escribir g de forma única como el producto de elementos $g = x_{p_1} \cdots x_{p_n}$, donde $x_{p_i} \in G$ es un p_i-elemento con $p_i \in \pi(o(g))$ para todo i y x_{p_i} conmuta con x_{p_j} para todo i, j tales que $p_i \neq p_j$. Con esta notación, decimos que x_{p_i} es la p_i-parte de g. Por otro lado, decimos que un grupo es un π-grupo si su orden es un π-número.

Ahora recordamos que un p-subgrupo de Sylow P de G es un p-subgrupo de G tal que su orden es la p-parte del orden de G. Denotamos por $\mathrm{Syl}_p(G)$ al conjunto de p-subgrupos de Sylow de G y por $\nu_p(G)$ al número de p-subgrupos de Sylow de G. Llamamos *números de Sylow* a la lista de números $\nu_p(G)$ donde $p \in \pi(G)$. Sea π un conjunto de primos. Análogamente, decimos que H es un π-subgrupo de Hall de G si H es un π-subgrupo de G tal que su orden es la π-parte del orden de G. Denotamos por $\mathrm{Hall}_\pi(G)$ al conjunto de π-subgrupos de Hall de G. Los resultados que aquí se usarán sobre la Teoría de Sylow o de Hall son bien conocidos y se usarán a menudo y en ocasiones sin hacer ninguna referencia explícita a ellos.

Dado un grupo G se llama *exponente* de G al mínimo común múltiplo de los órdenes de todos los elementos de G y se denota por $\exp(G)$. En particular, si G es un p-grupo, entonces $\exp(G)$ es el mayor de los órdenes de los elementos de G. En algunas situaciones utilizaremos la convención de la barra para denotar los grupos cocientes, es decir, dado un subgrupo normal N de un grupo G denotamos por $\overline{G}$ al grupo cociente G/N.

Recordamos que un grupo G es metabeliano (respectivamente metacíclico) si existe un subgrupo normal abeliano N (resp. cíclico) tal que el cociente G/N es también abeliano (resp. cíclico).

Dados dos elementos $x, y \in G$, definimos el *conmutador* $[x, y] = x^{-1}y^{-1}xy$. Al subgrupo generado por los conmutadores G', lo llamaremos *subgrupo derivado o conmutador*. Así, podemos definir la serie derivada de G, en la que cada término es el derivado del anterior. Se dice que G es *resoluble* si existe algún término de esta serie igual al subgrupo identidad.

Un grupo G se llama π*-resoluble*, donde π es un conjunto de primos, si existe una serie normal (es decir cada N_i es normal en G)

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$$

tal que cada factor N_i/N_{i-1} es un π-grupo resoluble o un π'-grupo. De forma similar, definimos la π-separabilidad. Un grupo G es π*-separable*, donde π es un conjunto de primos, si existe una serie normal tal que cada factor N_i/N_{i-1} es un π-grupo o un π'-grupo. En particular, dado un primo p, un grupo G es p*-resoluble* si tiene una serie normal donde cada factor es un p-grupo o un p'-grupo. En este caso, como los p-grupos son resolubles, la definición de p-separabilidad y p-resolubilidad coinciden. También coincidirán en el caso que $|\pi| = 2$ ya que, por el Teorema de Burnside [**24**, p. 216], sabemos que los grupos que tienen orden divisible por tan solo dos primos son resolubles. Además, si los factores de alguna serie normal son cíclicos, entonces el grupo es *superresoluble*.

Existe otra serie normal asociada a conmutadores: la *serie central descendente*. Se define $\gamma_1(G) = G$, $\gamma_2(G) = [G, G] = G'$, $\gamma_3(G) = [\gamma_2(G), G]$ y, así sucesivamente, $\gamma_{c+1}(G) = [\gamma_c(G), G]$ para cualquier $c \geq 1$. Se dice que G es *nilpotente* si existe un c tal que $\gamma_{c+1}(G) = 1$, en tal caso, llamamos *clase de nilpotencia* de G al menor de tales enteros c. A la intersección de todos los miembros de esta serie central descendente se le conoce como *residual nilpotente*. De hecho, es el menor subgrupo normal con grupo cociente nilpotente. La definición de nilpotencia dada es equivalente a que la siguiente serie, conocida como serie central ascendente, alcance G. Denotamos por $Z_0(G) = 1$, $Z_1(G) = \mathbf{Z}(G)$ el centro del grupo G y, sucesivamente, $Z_i(G)/Z_{i-1}(G) = \mathbf{Z}(G/Z_{i-1}(G))$. La serie formada por los $\{Z_i(G)\}_{i\geq 1}$ es la llamada *serie central ascendente* y, se sabe que $\gamma_{c+1}(G) = 1$ si y solo si $Z_c(G) = G$.

El concepto central del Capítulo 3 es la nilpotencia. Por ello, vamos a recordar algunas caracterizaciones de este concepto que son muy conocidas y de las que haremos uso, en general, sin hacer ninguna referencia al siguiente teorema.

Teorema 1.1. *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

(i) *G es nilpotente.*
(ii) *$\mathbf{N}_G(H) > H$ para todo subgrupo propio $H < G$.*
(iii) *Todo subgrupo maximal de G es normal.*
(iv) *Todo subgrupo de Sylow de G es normal. Por tanto, el grupo G es un producto directo de subgrupos de Sylow.*
(v) *Para cualquier conjunto de primos π, el grupo G es un producto directo de un π-grupo y un π'-grupo.*
(vi) *Si x, y son dos elementos de G que tienen orden coprimo, entonces x conmuta con y.*

Siguiendo la línea de la afirmación (vi) del teorema anterior, veremos en los siguientes capítulos nuevas caracterizaciones para grupos nilpotentes (y para resolubles), basadas esencialmente en relaciones entre el producto de los órdenes de dos elementos y el orden de su producto.

Dado un grupo G y $p \in \pi(G)$, denotamos por $\mathbf{O}_p(G)$ al mayor p-subgrupo normal de G. Definimos el *subgrupo de Fitting*, $\mathbf{F}(G)$, como el producto directo de los subgrupos $\mathbf{O}_p(G)$ con p recorriendo los divisores primos de G. Se tiene que $\mathbf{F}(G)$ es el mayor subgrupo normal nilpotente de G. Por otro lado, $\mathbf{O}^p(G)$ denota el menor subgrupo normal de G tal que el cociente $G/\mathbf{O}^p(G)$ es un p-grupo.

Por otro lado, el *socle* de un grupo G es el subgrupo generado por todos los subgrupos normales minimales de G. Recordamos que si $\mathbf{F}(G) = 1$ y llamamos S al socle de G, entonces S es el producto directo de los subgrupos normales minimales de G y $\mathbf{C}_G(S) = 1$.

Dado un grupo G y un subgrupo normal N de G, decimos que un subgrupo H de G es un *complemento* para N en G si $G = HN$ y $H \cap N = 1$. Un resultado que usaremos con frecuencia es el Teorema de Schur-Zassenhaus.

Teorema 1.2 (Schur-Zassenhaus). *Si G es un grupo y N un subgrupo de Hall normal de G entonces N posee complementos en G. Además, dos complementos cualesquiera son conjugados en G.*

Unos grupos muy conocidos en Teoría de Grupos y que aparecerán en varias ocasiones son los grupos de Frobenius. Comenzamos definiendo la *acción de Frobenius*. Sean A y N grupos tales que A actúa vía automorfismos sobre N. Decimos que la acción de A sobre N es de Frobenius si $x^a \neq x$ para cualesquiera $x \in N - \{1\}$ y $a \in A - \{1\}$. Decimos que un grupo G es *de Frobenius* si existen $A \leq G$, $N \trianglelefteq G$ tales que $G = AN$, $A \cap N = 1$ y la acción de A sobre N por conjugación es de Frobenius. El subgrupo N se llama *núcleo de Frobenius* y A *complemento de Frobenius*. Esto es, $G = AN$ es un grupo de Frobenius con núcleo N y complemento A si $\mathbf{C}_N(a) = 1$ para todos los elementos no triviales $a \in A$, equivalentemente, si $\mathbf{C}_G(x) \leq N$ para todo $1 \neq x \in N$.

Otros resultados muy utilizados y conocidos son el Lema de Hall-Higman y el Argumento de Frattini.

TEOREMA (Hall-Higman 1.2.3). Sea π un conjunto de primos. Sea G un grupo π-separable, y suponemos que $\mathbf{O}_{\pi'}(G) = 1$. Entonces $\mathbf{C}_G(\mathbf{O}_\pi(G)) \leq \mathbf{O}_\pi(G)$.

TEOREMA (Argumento de Frattini). Sean G un grupo, $N \trianglelefteq G$ y $P \in \mathrm{Syl}_p(N)$. Entonces $G = \mathbf{N}_G(P)N$.

Recordamos también el siguiente resultado sobre invarianza de subgrupos que usaremos en alguna ocasión sin referenciar. Dados A y G grupos de forma que A actúa via automorfismos sobre G y $(|A|, |G|) = 1$, entonces G tiene un p-subgrupo de Sylow que es A-invariante, para cada primo p. Además, en la misma situación, si P_1 y P_2 son p-subgrupos de Sylow A-invariantes de G, entonces $P_1^c = P_2$ para algún elemento $c \in \mathbf{C}_G(A)$.

Se dice que un grupo no trivial G es *simple* si no tiene subgrupos normales propios no triviales. Recordamos que los *grupos simples minimales* son grupos simples no abelianos en los que todo subgrupo propio es resoluble. A continuación, mostramos la clasificación de los grupos simples minimales, obtenida por Thompson en [40].

TEOREMA 1.3. *Sea G un grupo simple minimal. Entonces G es uno de los siguientes grupos:*

(i) $\mathrm{PSL}(2, 2^p)$*, donde p es un primo.*
(ii) $\mathrm{PSL}(2, 3^p)$*, donde p es un primo impar.*
(iii) $\mathrm{PSL}(2, p)$*, donde* $p > 3$ *es un primo tal que* $p^2 + 1 \equiv 0 \pmod{5}$.
(iv) $\mathrm{Sz}(2^p)$*, donde p es un primo impar.*
(v) $\mathrm{PSL}(3, 3)$.

Un grupo G es *almost-simple* si contiene un grupo simple S no abeliano tal que $S \leq G \leq \mathrm{Aut}(S)$. Recordamos que G es un grupo *quasisimple* si es perfecto ($G' = G$) y el cociente por su centro es simple. Por supuesto, si G es quasisimple tiene un único grupo simple no abeliano $G/\mathbf{Z}(G)$ como factor de composición. También es cierto que, para cada grupo simple no abeliano S, existe un único grupo G quasisimple de orden máximo tal que $G/\mathbf{Z}(G) \cong S$. A este grupo G se le llama *recubrimiento de Schur* de S y a $\mathbf{Z}(G)$ se le llama *multiplicador de Schur* de S [24, p. 272].

Otros grupos de interés son los extraespeciales. Previamente, recordamos que dado un grupo G, el *subgrupo de Frattini* $\Phi(G)$ de G es la intersección de todos los subgrupos maximales de G. Además, sabemos que $\Phi(G)$ es nilpotente. Ahora, dado un primo p, decimos que un p-grupo P es extraespecial si $\mathbf{Z}(P) = P' = \Phi(P)$ es un subgrupo cíclico de orden p. Para cada potencia p^{2m+1} hay dos grupos extraespeciales no isomorfos de ese orden. Si $p > 2$, uno de ellos tiene exponente p y el otro exponente p^2. En el caso que $p > 2$ y G tenga exponente p, vamos a recordar cómo son ciertos automorfismos de estos grupos, que denotaremos $E_{p^{2m+1}}$. Denotamos $Z = \mathbf{Z}(P)$ y $\mathrm{Aut}_Z(P)$ el grupo de automorfismos de P que son la identidad cuando los restringimos a Z. Por [**43**, Teorema 1], sabemos que $\mathrm{Aut}_Z(P)$ es un producto semidirecto IS, donde $I = \mathrm{Inn}(P) \cong P/Z$ es de orden p^{2m} y $S \cong \mathrm{Sp}(2m, p)$. En el caso que $m = 1$, se tiene por el Lema 9.12 del Capítulo 2 de [**21**] que $\mathrm{Sp}(2, q) \cong \mathrm{SL}(2, q)$.

A continuación, definimos los *automorfismos de tipo cuerpo* para los grupos simples $\mathrm{PSL}(2, q)$, con $q = 2^f$. Denotamos $G = \mathrm{GL}(2, q)$ y $H = \mathrm{SL}(2, q) = \mathrm{PSL}(2, q)$. Escribimos $F = \mathbb{F}_q$ para denotar el cuerpo de Galois de q elementos. Sea φ el automorfismo de Frobenius $\varphi : F \to F$ dado por $\varphi(a) = a^2 \in F$ para todo $a \in F$. Tenemos que $\varphi \in \mathrm{Gal}(F/\mathbb{F}_2)$.

El automorfismo de Frobenius φ induce un automorfismo de G aplicando φ a cada entrada de la matriz $x \in H$ (también en G). Se puede ver que si sumergimos $H \lhd \mathrm{Aut}(H)$, tenemos que $\langle \varphi \rangle \cap H = 1$. Los automorfismos en $\langle \varphi \rangle$ se llaman automorfismos de tipo cuerpo.

Como es usual, con x^G denotamos la clase de conjugación de x en G, donde G es un grupo y x un elemento de G.

Acabamos esta sección con la definición de un carácter. Dado un grupo G, una *representación* de G es un homomorfismo $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ para algún $n \in \mathbb{N}$. La aplicación de G en los números complejos definida por $\chi(x) = \mathrm{tr}\, \mathfrak{X}(x)$ para todo $x \in G$, donde tr denota la traza, se llama *carácter (ordinario)* asociado a la representación $\mathfrak{X}$. Dado que los caracteres no aparecen muy frecuentemente en esta memoria, no incluiremos en este capítulo ningún resultado sobre ellos. Sin embargo, en el Apéndice A nos serán de gran utilidad para probar el resultado principal. También haremos uso de ellos en el Capítulo 5. Por ello, remitimos al lector al libro de Isaacs [**23**] para ampliar cualquier información o resultado que aquí no se mencione y que sea necesario para la comprensión de la misma.

Capítulo 2

Origen de los resultados

2.1. Introducción

Como consecuencia de su clasificación de los grupos simples minimales, Thompson en [**40**] demostró que un grupo G es resoluble si y solo si no existen elementos no triviales $x, y, z \in G$ de órdenes coprimos dos a dos tales que $xyz = 1$. En 2015, Guralnick y Tiep [**18**] probaron que para garantizar la resolubilidad basta suponer la no existencia de tales elementos de orden potencia de primo. Motivados por este resultado, uno de los objetivos de esta tesis es obtener la versión para elementos de orden potencia de primo del Teorema de Baumslag y Wiegold [**5**], el cual afirma que un grupo G es nilpotente si y solo si para todo par de elementos $x, y \in G$ de orden coprimo, se tiene que $o(xy) = o(x)o(y)$.

La segunda sección de este capítulo es una recopilación de diferentes resultados conocidos en los que a partir de información sobre los órdenes de ciertos productos de elementos, se obtiene información sobre la estructura del grupo o se caracteriza la pertenencia de un elemento dado a un subgrupo normal relevante. La demostración del Teorema 2.2 se puede encontrar en [**3**]. En la tercera sección continuamos en la línea anterior, enunciamos el Teorema de Thompson y las diferentes versiones que prueban Guralnick y Tiep. Las demostraciones de las nuevas versiones que presentamos se pueden encontrar en [**33**]. Por último, damos la prueba original del Teorema de Baumslag y Wiegold mencionado antes y comentamos las primeras ideas que surgen a partir de dicho teorema.

2.2. Antecedentes generales

En 1954, L. J. Paige formula una pregunta relacionada con los órdenes de ciertos elementos. Este pregunta ha servido de motivación durante muchos años.

Cuestión (Paige). Sean G un grupo y $P \in \mathrm{Syl}_2(G)$. ¿Es cierto que toda coclase no trivial Pg debe contener algún elemento de orden impar?

Es fácil ver que si G es resoluble entonces cada coclase no trivial de $P \in \mathrm{Syl}_2(G)$ contiene al menos un elemento de orden impar. Sin embargo, la pregunta de Paige fue respondida negativamente por Thompson [**41**], en 1967, dando como ejemplo los grupos $\mathrm{SL}(2, q)$ con $q \equiv 5 \pmod 8$. Por tanto, una coclase no trivial de un 2-subgrupo de Sylow puede contener solo elementos de orden par.

A raíz de la cuestión de Paige, en 1962, G. Zappa [**44**] lanza la siguiente pregunta.

Cuestión (Zappa). Sea p un primo. ¿Hay algún grupo G con alguna coclase no trivial Pg, con $P \in \mathrm{Syl}_p(G)$, que contiene solo elementos cuyos órdenes son potencias de p?

En [**13**] D. Goldstein y Guralnick dieron más contraejemplos a la pregunta de Paige y volvieron a reformular la pregunta de Zappa. En el caso $p = 2$, una respuesta afirmativa a la pregunta de Zappa da un contraejemplo en un sentido muy fuerte a la pregunta de Paige. En [**8**] M. Conder da respuestas afirmativas a las preguntas de Zappa pero para $p = 5$ y P cíclico de orden 5.

Uno de los resultados principales relacionados con órdenes de productos es el Teorema de Baer-Suzuki [**21, 37**]. El enunciado que aquí damos es de un artículo de J. Alperin y R. Lyons [**2**].

Teorema 2.1 (Baer-Suzuki). *Sea p un primo y sea G un grupo. Un p-elemento $x \in G$ es tal que $x \in \mathbf{O}_p(G)$ si y solo si $\langle x, x^g \rangle$ es un p-subgrupo de G para todo $g \in G$.*

En vista de este resultado, es natural preguntarse si es cierto que en un grupo G, dado un primo p que divide a $|G|$ y un p-elemento $x \in G$, se cumple que xx^g es un p-elemento para todo $g \in G$ si y solo si $x \in \mathbf{O}_p(G)$. La respuesta a esta pregunta es negativa. Sea $q \equiv 1 \pmod p$, con p, q primos impares. Sea $G = P[Q]$ un grupo de Frobenius con $P = \langle x \rangle$ de orden p y $|Q| = q$. Entonces $x^G = xQ$ y para todo $g \in G$ se tiene que $xx^g = x(xy) = x^2y$ para algún $y \in Q$. Como $x^2y \notin Q$, $x^2y = xx^g$ es un p-elemento.

El siguiente teorema es el primero de los resultados originales de esta memoria y aparece como Teorema A en [**3**]. Además, marca el estilo de resultados que aquí se probarán, aunque con la diferencia de que en adelante obtendremos propiedades del grupo en términos del orden del producto de dos elementos de órdenes coprimos.

Teorema 2.2. *Sean G un grupo, p un primo y $x \in G$ un p-elemento. Entonces xy es un p-elemento para todo p-elemento $y \in G$ si y solo si $x \in \mathbf{O}_p(G)$.*

La demostración de este resultado es una consecuencia inmediata de la siguiente variante del Teorema de Baer-Suzuki, llevada a cabo por Guralnick y G. R. Robinson.

Teorema 2.3 (Corolario B de [**17**]). *Sean G un grupo y p un primo. Sea X un p-subgrupo de G tal que $[x, g]$ es un p-elemento para todo $x \in X$ y $g \in G$. Entonces $X \leq \mathbf{O}_p(G)$.*

Este teorema, a diferencia del de Baer-Suzuki, depende de la Clasificación de los Grupos Simples Finitos.

Demostración del Teorema 2.2. Suponemos que $x \in \mathbf{O}_p(G)$. Como x está en todos los p-subgrupos de Sylow de G, es inmediato que xy es un p-elemento para todo p-elemento y de G. Recíprocamente, suponemos que xy es un p-elemento para todo p-elemento y de G. Entonces, en particular, xx^g es un p-elemento para todo $g \in G$. De la misma forma, $x^2x^g = x(xx^g)$ es un p-elemento para todo $g \in G$. Similarmente, obtenemos que x^ix^g y $(x^i)^{-1}(x^i)^g$ son p-elementos para todo $g \in G$ y para todo entero i. Por tanto, $[x^i, g]$ es un p-elemento para todo $x^i \in \langle x \rangle$, y aplicando el Teorema 2.3, obtenemos $x \in \mathbf{O}_p(G)$. □

En vista del teorema anterior, podemos preguntarnos si también es cierta la tesis debilitando la hipótesis de forma que p divida a $o(xy)$ en lugar de que sea p-elemento.

Cuestión 1. Sean G un grupo, p un primo y $x \in G$ un p-elemento. ¿Es cierto que si p divide a $o(xy)$ para todo p-elemento $y \in G$ con $y \neq x^{-1}$ entonces $x \in \mathbf{O}_p(G)$?

2.3. Teorema de Thompson y generalizaciones

Thompson, en el Corolario 3 de [**40**], establece que un grupo G es resoluble si y solo si no existen elementos no triviales $x, y, z \in G$ de orden coprimo dos a dos tales que $xyz = 1$. En este resultado y en los siguientes de esta sección, el trabajo reside en probar la resolubilidad, ya que la otra implicación es bien sencilla (véase, por ejemplo, el Corolario 2.9). Hemos observado que este resultado se puede enunciar de forma equivalente, como podemos ver en el siguiente corolario.

Corolario 2.4 (Thompson). *Un grupo G es resoluble si y solo si para todo par de elementos no triviales $x, y \in G$ tales que $(o(x), o(y)) = 1$ se tiene que*

$$\pi(o(xy)) \cap \pi(o(x)o(y)) \neq \varnothing.$$

Demostración. Por el resultado de Thompson mencionado, tenemos que un grupo G no es resoluble si y solo si existen elementos no triviales $x, y, z \in G$ de orden coprimo dos a dos tales que $xy = z^{-1}$. En otras palabras, un grupo G no es resoluble si y solo si existen elementos no triviales $x, y \in G$ de orden coprimo tales que $o(xy)$ es coprimo con $o(x)o(y)$, es decir, $\pi(o(xy)) \cap \pi(o(x)o(y)) = \varnothing$. □

Guralnick y Tiep en el Teorema 1.1 de [**18**] demuestran que un grupo G es resoluble si y solo si $xyz \neq 1$ para todo $x, y, z \in G$ no triviales donde x es un p-elemento, y un q-elemento, z un r-elemento y p, q, r primos distintos. De hecho, veremos en el Apéndice A la siguiente versión de ese teorema.

Teorema 2.5. *Un grupo G es resoluble si y solo si $xyz \neq 1$ para todo $x, y, z \in G$ no triviales donde x es un 2-elemento, $o(y) = q$, $o(z) = r$, con $q \neq r$ primos impares.*

Una consecuencia inmediata de estos resultados es el siguiente corolario.

Corolario 2.6 (Guralnick-Tiep). *Un grupo G es resoluble si y solo si para todo par de elementos no triviales $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$ se tiene que*

$$\pi(o(xy)) \cap \pi(o(x)o(y)) \neq \varnothing.$$

Demostración. Vamos a ver que si un grupo G no es resoluble entonces existen elementos no triviales $x, y \in G$ de orden potencia de primo tales que $\pi(o(xy)) \cap \pi(o(x)o(y)) = \varnothing$. Por el resultado de Guralnick y Tiep sabemos que un grupo G no es resoluble si y solo si existen primos p, q, r y elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un r-elemento y $xyz = 1$. Este hecho es equivalente a que un grupo G no es resoluble si y solo si existen primos p, q, r y elementos no triviales $x, y \in G$ tales que x es un p-elemento, y es un q-elemento y $xy = z^{-1}$ es un r-elemento, lo cual implica que $(o(xy), o(x)o(y)) = 1$. □

Queremos notar que los resultados anteriores tan solo dependen de la clasificación de los grupos simples minimales. Sin embargo, el resto de resultados de esta sección utilizan la clasificación completa de los grupos finitos simples.

Dado un primo p, Guralnick y Tiep prueban también que un grupo G es p-resoluble si y solo si para todos los primos $q \neq r$ distintos de p y para todos los elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y un q-elemento y z un r-elemento, $xyz \neq 1$. Procediendo como en los corolarios anteriores, podemos escribir una versión ligeramente más débil de este resultado.

Corolario 2.7 (Guralnick-Tiep). *Sean p un primo y G un grupo. Entonces G es p-resoluble si y solo si para todo $q \neq p$ primo y para todo par de elementos no triviales $x, y \in G$ con x p-elemento e y q-elemento se tiene que*

$$\pi(o(xy)) \cap \pi(o(x)o(y)) \neq \varnothing.$$

Demostración. De nuevo, basta ver que si G no es p-resoluble entonces existe un primo $q \neq p$ y existen elementos no triviales $x, y \in G$ con x p-elemento e y q-elemento tales que $\pi(o(xy)) \cap \pi(o(x)o(y)) = \varnothing$. Por el resultado de Guralnick y Tiep tenemos que un grupo G no es p-resoluble si y solo si existen primos $q \neq r$ distintos de p y existen elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un r-elemento y $xyz = 1$. De nuevo, esto es equivalente a que un grupo G no es p-resoluble si y solo si existe un primo $q \neq p$ y existen elementos no triviales $x, y \in G$ tales que x es un p-elemento, y es un q-elemento y $xy = z^{-1}$ es un r-elemento, lo cual implica que $(o(xy), o(x)o(y)) = 1$. □

En el mismo artículo, Guralnick y Tiep conjeturaron que dados dos primos impares $q \neq p$, es equivalente que G tenga factores de composición de orden divisible por pq a que G contenga elementos x, y, z tales que x es un 2-elemento, y es un p-elemento, z es un q-elemento y $xyz = 1$ (Conjetura 6.2 de [**18**]). Esta conjetura ha sido probada por H. Lee en [**27**]. Dicha conjetura se puede unir a la caracterización de los grupos p-resolubles de Guralnick y Tiep y escribir de esta forma el resultado.

TEOREMA 2.8 (Guralnick-Tiep-Lee). *Sea G un grupo y sean p y q primos diferentes. Las siguientes afirmaciones son equivalentes:*

(i) *G contiene un factor de composición cuyo orden es divisible por pq.*
(ii) *Existen elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un r-elemento para algún primo $r \neq p, q$ y $xyz = 1$. Además, si p y q son impares, podemos tomar $r = 2$.*

La mayor parte del trabajo para demostrar este teorema está en el caso quasisimple. En el Apéndice A, veremos la reducción a grupos quasisimples de este teorema, siguiendo las ideas de [**18**] y [**27**].

De nuevo, reescribimos una versión más débil del Teorema 2.8.

COROLARIO 2.9. *Sea G un grupo y sean $p \neq q$ primos. Las siguientes afirmaciones son equivalentes:*

(i) *G tiene factores de composición de orden divisible por pq.*
(ii) *Existen elementos $x, y \in G$ con $1 \neq x$ un p-elemento, $1 \neq y$ un q-elemento tales que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$.*

DEMOSTRACIÓN. Suponemos que G contiene un factor de composición cuyo orden es divisible por pq. Por el Teorema 2.8, existen elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un r-elemento para algún primo $r \neq p, q$ y $xyz = 1$. Por tanto, $z = (xy)^{-1}$ y se sigue que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$.

Suponemos ahora que existen elementos no triviales $x, y \in G$ con x un p-elemento, y un q-elemento de forma que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$. Queremos probar que G contiene un factor de composición cuyo orden es divisible por pq.

Sea G un contraejemplo minimal. Como el orden de G es divisible por pq y G no tiene factores de composición de orden divisible por pq, deducimos que G no es simple. Sea N un subgrupo normal propio no trivial de G. Observamos que G/N tampoco puede contener un factor de composición de orden divisible por pq. Para llegar a contradicción comenzamos suponiendo que $x \in N$. Sea $z = (xy)^{-1}$. Esto implica que $xyz = 1$. Así $yz = x^{-1} \in N$ y tenemos que $yzN = N$. Deducimos que $yN = z^{-1}N$. Como $\pi(o(x)o(y)) \cap \pi(o(xy))) = \varnothing$, tenemos que $(o(y), o(z^{-1})) = 1$ y, entonces, $o(yN) = o(z^{-1}N) = 1$. Por tanto, $y \in N$ y así N es un contraejemplo de orden menor que G. Contradicción. De la misma forma, si $x \notin N$, obtenemos que $y \notin N$. En este caso $xN \in G/N$ es un p-elemento no trivial, $yN \in G/N$ es un q-elemento no trivial y $o(xyN)$ es coprimo a pq (ya que $o(xyN)$ es un divisor de $o(xy)$, el cual es coprimo a p y a q). De nuevo, tenemos una contradicción con la minimalidad de G. □

Observamos que este corolario dice que si G es simple de orden divisible por pq, entonces existen $1 \neq x$ p-elemento, $1 \neq y$ q-elemento tales que $\pi(o(xy)) \cap \pi(o(x)o(y)) = \varnothing$. Nos preguntamos si es cierta la siguiente versión más fuerte.

Conjetura 2.10. *Sea G un grupo simple. Sean $p \neq q$ dos primos divisores de $|G|$. Sea $x \in G$ un p-elemento no trivial. Entonces existe un q-elemento no trivial $y \in G$ tal que $o(xy)$ es coprimo con pq.*

Para probar los resultados del Capítulo 4, utilizaremos la siguiente versión de esta conjetura.

Conjetura 2.11. *Suponemos que $G = \langle x \rangle S$ es un grupo almost-simple con socle S, donde $x \in G$ es no trivial. Entonces para todo $p \in \pi(G) - \pi(o(x))$, existe un p-elemento $y \in G$ no trivial tal que p no divide a $o(xy)$.*

Observamos que probar la Conjetura 2.11, significa probar el enunciado para cada par (S, x) donde S es simple y $x \in \mathrm{Aut}(S)$. Nótese que en la Conjetura 2.11 únicamente necesitamos que en el producto xy no aparezca uno de los primos, en lugar de que no aparezca ninguno de los dos, por tanto, estamos debilitando la tesis. Por otro lado, al no exigir que x sea un elemento de orden potencia de primo ni que G sea simple, estamos haciendo más débil la hipótesis. Estas conjeturas parecen más profundas que el Teorema 2.8 ya que en vez de encontrar elementos x e y que cumplan cierta condición, requiere encontrar un y para cada x.

Teorema 2.12. *La Conjetura 2.11 es cierta si el socle S de G es un grupo alternado, un grupo esporádico o un grupo simple de tipo Lie en característica coprima con $o(x)$.*

Por tanto, la Conjetura 2.11 es cierta salvo quizás para los grupos cuyo socle es un grupo simple de tipo Lie en característica no coprima con $o(x)$. En el Apéndice A, probaremos el Teorema 2.12 en los casos que S es esporádico o alternado. El caso de tipo Lie podemos encontrarlo en [**3**] y no se ha incluido aquí por la complejidad de las pruebas. Sin embargo, para ilustrar parte de las ideas de ese caso, probaremos el Teorema 2.5.

Para acabar, queremos mencionar el siguiente ejemplo.

Ejemplo 2.13. Sean $G = \mathsf{A}_8$, el grupo alternado de grado 8, $p = 3$, $x = (1, 2)(3, 4)(5, 6)(7, 8)$ e $y = (1, 2, 3)$. Entonces el orden de xy^g es divisible por 6 para todo $g \in G$. Sin embargo, G tiene otra clase de p-elementos no triviales donde sí podemos encontrar un elemento y adecuado y, por ello, A_8 no es un contraejemplo de la Conjetura 2.11.

2.4. Teorema de Baumslag y Wiegold

Esta sección está dedicada al Teorema de Baumslag y Wiegold que ha sido el origen de todos los resultados de esta memoria. En primer lugar, vamos a presentar su demostración original.

TEOREMA 2.14 (Baumslag-Wiegold). *Sea G un grupo. Se tiene que G es nilpotente si y solo si $o(xy) = o(x)o(y)$ para todo $x, y \in G$ con $(o(x), o(y)) = 1$.*

DEMOSTRACIÓN. Sea G un grupo nilpotente. Entonces para todos los elementos $x, y \in G$ tales que $(o(x), o(y)) = 1$ se tiene que $xy = yx$, por el Teorema 1.1. Esto implica inmediatamente que $o(xy) = o(x)o(y)$.

Suponemos ahora que para todo $x, y \in G$ con $(o(x), o(y)) = 1$ se cumple que $o(xy) = o(x)o(y)$. Observamos que esta condición se puede extender a más de dos elementos por inducción, por tanto, $o(x_1 \cdots x_n) = o(x_1) \cdots o(x_n)$, para todo $x_i \in G$ tales que $(o(x_i), o(x_j)) = 1$ para todo $i \neq j$. Queremos ver que G es nilpotente, para ello vamos a ver que todo p-subgrupo de Sylow de G es normal, para todo primo p que divide a $|G|$.

Sea $\pi(G) = \{p_1, \ldots, p_r\}$ y sea $P_i \in \mathrm{Syl}_{p_i}(G)$ para $i \in \{1, \ldots, r\}$. Queremos probar que $G = P_1P_2 \cdots P_r$. Para ello, vamos a ver, en primer lugar, que cualquier elemento $x \in P_1P_2 \cdots P_r$ se puede escribir de forma única como $x = s_1 \cdots s_r$, con $s_i \in P_i$ para todo i. Sea $x \in P_1P_2 \cdots P_r$. Suponemos que $x = s_1s_2 \cdots s_r = t_1t_2 \cdots t_r$, con $s_i, t_i \in P_i$ para todo i. Entonces $s_1s_2 \cdots s_{r-1} = t_1t_2 \cdots t_rs_r^{-1}$. Si $t_rs_r^{-1} \neq 1$, entonces por hipótesis, el elemento $t_1t_2 \cdots t_rs_r^{-1}$ tiene orden divisible por p_r, mientras que $s_1s_2 \cdots s_{r-1}$ no. Por tanto, llegamos a una contradicción que implica que $t_rs_r^{-1} = 1$. Entonces $s_r = t_r$. Repitiendo el proceso, deducimos que $s_i = r_i$ para todo i. Sea $\sigma : P_1 \times \cdots \times P_r \to P_1P_2 \cdots P_r$, la aplicación que a $(s_1, \ldots, s_r)$ le asocia el elemento $s_1 \cdots s_r$, donde $P_1 \times \cdots \times P_r$ denota el producto cartesiano de los subgrupos P_i. Hemos visto que σ es biyectiva. Por tanto, $|P_1 \cdots P_r| = |G|$ y entonces $G = P_1 \cdots P_r$.

Para concluir, sea x un conjugado de un elemento cualquiera de P_1. Entonces, por la igualdad anterior, $x = s_1s_2 \cdots s_r$ con $s_i \in P_i$ para todo i. Como x tiene orden potencia de p_1, entonces $s_2 = s_3 = \cdots = s_r = 1$ y deducimos que $x \in P_1$. Esto implica que P_1 es normal en G. Repetimos el proceso para todo $i \in \{2, \ldots, r\}$ y obtenemos que P_i es normal para todo $i \in \{1, \ldots, r\}$. Concluimos que G es nilpotente. □

Queremos recalcar que dada la gran cantidad de caracterizaciones que se conocen sobre grupos nilpotentes, nos pareció sorprendente que este resultado no fuese conocido o consecuencia inmediata de alguna de ellas. Por ejemplo, uno podría pensar que dados dos elementos $x, y \in G$ es equivalente que $xy = yx$ a que $o(xy) = o(x)o(y)$, en cuyo caso el Teorema 2.14 se seguiría inmediatamente de la Caracterización (vi) del Teorema 1.1. Vamos a ver con el siguiente ejemplo que si dos elementos $x, y \in G$ de órdenes coprimos cumplen que $o(xy) = o(x)o(y)$, esto no implica que $xy = yx$.

Ejemplo 2.15. Consideramos $G = F_{42}$ el grupo de Frobenius de orden 42 generado por un un elemento a de orden 6 y un elemento b de orden 7. La acción de a sobre b es por conjugación de forma que $b^a = b^5$.

Podemos encontrar dos elementos x, y tales que $o(xy) = o(x)o(y)$ pero estos no conmutan. Sean, por ejemplo, $x = a^4$ e $y = a^3b$ de forma que $o(x) = 3$ y $o(y) = 2$. Veamos que, en efecto, $o(y) = 2$.

$$y^2 = (a^3b)(a^3b) = a^6b^{a^3}b = b^6b = 1.$$

De forma análoga, podemos ver que $o(x) = 3$. Ahora, si computamos los productos xy e yx, observamos que $o(xy) = 6 = o(x)o(y)$ pero los elementos x e y no conmutan. En efecto,

$$xy = (a^4)(a^3b) = ab \neq ab^2 = (a^3b)(a^4) = yx,$$

donde en la penúltima igualdad hemos utilizado que $b^{a^4} = b^2$.

A continuación, vamos a estudiar las posibles formas de mejorar este resultado. Por ejemplo, la respuesta a la siguiente cuestión podría ser afirmativa.

Cuestión 2. ¿Es cierto que si para todo $x, y \in G$ tales que $(o(x), o(y)) = 1$ se cumple que $o(x)o(y) \leq o(xy)$, entonces G es nilpotente?

En segundo lugar, nos preguntamos si es cierto que un grupo G es nilpotente si y solo si $o(x)o(y)$ divide a $o(xy)$ para todo $x, y \in G$ con $(o(x), o(y)) = 1$. Este resultado será consecuencia del Teorema A del Capítulo 3.

La familia de grupos que cumplen las relaciones contrarias, es decir, $o(xy) \leq o(x)o(y)$ para todos los elementos $x, y \in G$ con $(o(x), o(y)) = 1$ u $o(xy)$ divide a $o(x)o(y)$ para todos los elementos $x, y \in G$ con $(o(x), o(y)) = 1$, son mucho más amplias y parece difícil clasificar los grupos que cumplen estas propiedades. Veremos en la Sección 3.5 la dificultad de clasificar los grupos que cumplen una condición similar.

Otra posible generalización del Teorema de Baumslag y Wiegold es considerar solo elementos de orden potencia de primo. Esto aparece como Corolario B en el Capítulo 3. Se puede observar que el desarrollo de la prueba del Teorema de Baumslag y Wiegold no es válido para probar esta versión ya que en este caso la propiedad no se extendería al producto de más de dos elementos.

En el próximo capítulo, empezamos a desarrollar las ideas mencionadas en esta sección.

Capítulo 3

Nilpotencia y subgrupos de Hall

3.1. Introducción

El primer resultado principal es una caracterización de los grupos nilpotentes al estilo de las de Thompson, Guralnick y Tiep para grupos resolubles.

TEOREMA A. *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

(i) *G es nilpotente.*

(ii) *Para todos los elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$,*
$$\pi(o(x)o(y)) = \pi(o(xy)).$$

(iii) *Para todos los elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$,*
$$\pi(o(x)o(y)) \subseteq \pi(o(xy)).$$

Como consecuencia de este resultado obtenemos la versión del Teorema de Baumslag y Wiegold mencionada en la Sección 2.4.

COROLARIO B. *Un grupo G es nilpotente si y solo si se cumple que $o(xy) = o(x)o(y)$ para todo $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$.*

El teorema anterior, como el de Baumslag y Wiegold, es elemental.

El segundo objetivo se basa en restringir la hipótesis del Teorema A a los π-elementos de G, donde π es un conjunto de primos. De esta forma, se obtiene información sobre la existencia de π-subgrupos de Hall nilpotentes.

TEOREMA C. *Sea π un conjunto de primos divisores del orden de un grupo G. Suponemos que para todos los π-elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$, se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. Entonces G tiene π-subgrupos de Hall nilpotentes.*

Este resultado es más profundo y depende de la Clasificación de los Grupos Simples Finitos por medio del Corolario 2.9.

Debemos notar que el recíproco de este teorema no es cierto: por ejemplo $G = \mathrm{PSL}(2, 16)$ tiene un $\{3, 5\}$-subgrupo de Hall abeliano pero existen elementos $x, y \in G$ tales que $o(x) = 3$, $o(y) = 5$ y $o(xy) = 17$.

Sin embargo, el recíproco es cierto para grupos π-separables.

Teorema D. *Sea π un conjunto de primos divisores de $|G|$, donde G es un grupo π-separable. Las siguientes afirmaciones son equivalentes:*

(i) *Para todos los π-elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$, se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$.*

(ii) *G tiene π-subgrupos de Hall nilpotentes.*

En vista del Teorema A, parece natural pensar que, quizás, la condición "para todos los π-elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$, se tiene que $\pi(o(x)o(y)) = \pi(o(xy))$" es también equivalente a (i) y (ii) del Teorema D. Sin embargo, veremos que $G = C_6[E_{5^3}]$ es un contraejemplo.

Por último, siguiendo la línea del Teorema A y dado un conjunto de primos π que dividen al orden de un grupo, obtenemos una versión local que caracteriza la existencia de un π-subgrupo de Hall normal.

Teorema E. *Sea G un grupo y sea $\pi \subseteq \pi(G)$. Entonces las siguientes afirmaciones son equivalentes:*

(i) *Para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.*

(ii) *G tiene un π-subgrupo de Hall normal.*

Vamos a dividir las demostraciones de los teoremas anteriores en las Secciones 3.3 y 3.4. En la primera de ellas probamos los Teoremas A, C y D y en la segunda, el Teorema E. La Sección 3.2 está destinada a mostrar los resultados necesarios para probar los teoremas anteriores, mientras que en la Sección 3.5 recogemos algunas cuestiones y resultados derivados de los teoremas de las secciones previas.

Los resultados de este capítulo forman los artículos [**4**] y [**33**].

3.2. Resultados específicos

Esta sección contiene algunos resultados necesarios para probar los teoremas expuestos en la introducción. En primer lugar, recordamos un resultado de P. Hall [**19**] que nos permitirá probar que los grupos sin factores de composición de orden divisible por pq tienen $\{p, q\}$-subgrupos de Hall. De hecho, veremos más. Como es usual, dado un conjunto de primos π, decimos que un grupo G satisface D_π si G tiene π-subgrupos de Hall, si cualquier par de π-subgrupos de Hall son conjugados y si todo π-subgrupo de G está contenido en algún π-subgrupo de Hall.

Lema 3.1. *Sea π un conjunto de primos. Sean G un grupo y $N \trianglelefteq G$. Si N tiene un π-subgrupo de Hall nilpotente, G/N satisface D_π y G/N tiene π-subgrupos de Hall resolubles, entonces G satisface D_π.*

Para nuestro objetivo, usaremos la siguiente consecuencia del lema anterior.

Corolario 3.2. *Sean p y q primos. Sea G un grupo sin factores de composición de orden divisible por pq. Entonces G satisface D_π, donde $\pi = \{p, q\}$. En particular, si G es p-resoluble, entonces G satisface $D_{\{p,r\}}$ para todo primo r.*

Demostración. Sea G un contraejemplo minimal. Si G es simple, p o q no divide a $|G|$ y el resultado se sigue de los teoremas de Sylow. Por tanto, podemos suponer que G no es simple. Sea N un subgrupo normal minimal de G. Como la hipótesis se hereda a grupos cocientes, G/N satisface D_π. Por el Teorema de Burnside, los π-subgrupos de Hall de G/N son resolubles. Por hipótesis, p o q no divide a $|N|$, así N tiene π-subgrupos de Hall nilpotentes (de hecho, son subgrupos de Sylow.) Por el lema previo, G satisface D_π. Esto es una contradicción. □

A continuación, vamos a recordar algunos términos que nos serán de utilidad. En primer lugar, recordamos que un grupo G es *no nilpotente minimal* si G no es nilpotente pero todo subgrupo propio de G es nilpotente. Utilizaremos el siguiente resultado que se puede encontrar en [**34**, 9.1.9].

Lema 3.3 (O. J. Schmidt). *Sea G un grupo no nilpotente minimal. Entonces $G = PQ$ donde $P \in \mathrm{Syl}_p(G)$ es cíclico y $Q \in \mathrm{Syl}_q(G)$ es normal en G, con $q \neq p$ primos.*

Recordamos también que un grupo G se dice que es *p-cerrado* si tiene un p-subgrupo de Sylow normal. De forma análoga, hemos definido los grupos *π-cerrados*, que son aquellos que tienen un π-subgrupo de Hall normal, para π un conjunto de primos que dividen al orden de G. Diremos que G es *no-p-cerrado minimal* (respectivamente *no-π-cerrado minimal*) si G no es *p-cerrado* (resp. *π-cerrado*) pero todo subgrupo propio de G es *p-cerrado* (resp. *π-cerrado*). Nos gustaría mencionar que se ha usado esta nomenclatura por concordancia con los grupos no nilpotentes minimales. Sin embargo, a nuestros grupos no-p-cerrados minimales también se les conoce como *inner p-closed*, como podemos ver, por ejemplo, en [**30**]. En dicho artículo los grupos no p-cerrados minimales son aquellos en los que todo subgrupo propio y toda imagen homomorfa es p-cerrada pero G no lo es.

Los grupos no-p-cerrados minimales no son necesariamente grupos p-resolubles, pero en el caso particular que lo sean, tenemos un resultado del tipo del Lema 3.3. El siguiente lema es el Lema 3.5 de [**33**].

Lema 3.4. *Sea G un grupo p-resoluble no-p-cerrado minimal. Entonces $|\pi(G)| = 2$, donde $\pi(G)$ es el conjunto de primos divisores de $|G|$.*

Demostración. Procedemos por reducción al absurdo. Suponemos que $|\pi(G)| \geq 3$. Sea P un p-subgrupo de Sylow de G. Sea $q \in \pi(G)$ con $q \neq p$. Como G es p-resoluble, el Corolario 3.2 nos garantiza que G satisface $D_{\{p,q\}}$. Por tanto, existe un $\{p, q\}$-subgrupo de Hall H de G tal que $P \leq H$. Como G es no-p-cerrado minimal, P es normal en H. Entonces H está contenido en $\mathbf{N}_G(P)$. Hemos visto que para cada $q \in \pi(G) - \{p\}$, se tiene que $\mathbf{N}_G(P)$ contiene un $\{p, q\}$-subgrupo de Hall de G. Por tanto, $\mathbf{N}_G(P) = G$. Esto es una contradicción. $\square$

Ahora, de forma análoga, dado un conjunto de primos π, caracterizamos los grupos no-π-cerrados minimales en el caso que sean π-separables. La siguiente proposición podemos encontrarla en [4].

PROPOSICIÓN 3.5. *Sea G un grupo π-separable no π-cerrado minimal con $\pi \subseteq \pi(G)$ no vacío. Entonces $\pi(G) = \pi \cup \{q\}$, con $q \in \pi(G) - \pi$.*

DEMOSTRACIÓN. Sea G un contraejemplo minimal. Podemos suponer que $|\pi| > 1$. En caso contrario, G es un no p-cerrado minimal y por el Lema 3.4, obtenemos que $|\pi(G)| = 2$.

Sea M un subgrupo normal maximal de G. Como G es π-separable, tenemos que G/M es π-grupo o π'-grupo. Suponemos primero que G/M es π'-grupo. Como M tiene un π-subgrupo de Hall normal H y G/M es π'-grupo, se tiene que H es un π-subgrupo de Hall de G. Además H es característico en M y, por tanto, H es normal en G, lo cual contradice la hipótesis.

Podemos suponer que G/M es π-grupo. Por hipótesis, M tiene un π-subgrupo de Hall normal que denotamos por H_0. De forma análoga al procedimiento realizado al final del párrafo anterior, observamos que H_0 es normal en G. Como G es π-separable, podemos escribir $H_0 = H \cap M$, para algún $H \in \mathrm{Hall}_\pi(G)$. Trabajamos con $\overline{G} = G/H_0$. Sea $\overline{L}$ un subgrupo propio de $\overline{G}$. Entonces L es un subgrupo propio de G y por hipótesis, L tiene un π-subgrupo de Hall normal que denotamos por K. Entonces $\overline{K}$ es un π-subgrupo de Hall normal de $\overline{L}$. Hemos probado así que todo subgrupo propio de $\overline{G}$ tiene un π-subgrupo de Hall normal. Además, $\overline{G}$ no tiene π-subgrupos de Hall normales, ya que en caso contrario, razonando como anteriormente, G tendría un π-subgrupo de Hall normal, lo cual es una contradicción. Por tanto, si $H_0 \neq 1$, por ser G contraejemplo minimal, tenemos que $\pi(G/H_0) = \pi \cup \{q\}$, con $q \in \pi(G/H_0) - \pi$. Como H_0 es un π-subgrupo de G, entonces $\pi(G) = \pi \cup \{q\}$, con $q \in \pi(G) - \pi$, lo cual contradice el hecho de que G es un contraejemplo.

Se puede suponer que $H_0 = H \cap M = 1$. Entonces tenemos que M es un π'-subgrupo de Hall normal de G. Se tiene que todo subgrupo propio de G que contiene a M, tiene un π'-subgrupo de Hall normal; y a su vez, por hipótesis tiene un π-subgrupo de Hall normal. Entonces todo subgrupo propio T de G que contiene a M es de la forma $T = M \times K$, con $K \in \mathrm{Hall}_\pi(T)$. Así, si $\pi = \{p_1, \ldots, p_r\}$ con $r \geq 2$, para cada $P_i \in \mathrm{Syl}_{p_i}(G)$ tenemos que el subgrupo propio $P_iM = P_i \times M$. Entonces $\langle P_1, \ldots, P_r \rangle \leq \mathbf{C}_G(M)$. Por tanto, $G = H \times M$, para algún $H \in \mathrm{Hall}_\pi(G)$ contenido en $\langle P_1, \ldots, P_r \rangle$, lo cual es una contradicción con el hecho de que G no tiene ningún π-subgrupo de Hall normal. $\square$

Nótese que en cualquiera de los resultados anteriores la condición de π-separabilidad es necesaria. Si tomamos $G = \mathsf{A}_5$ y $\pi = \{5\}$ (o $p = 5$), este grupo es no 5-cerrado minimal ya que todos sus subgrupos tienen un 5-subgrupo de Sylow normal pero $\pi(G) = \{2, 3, 5\}$, luego $|\pi(G)| > 2$. Esto no contradice el resultado ya que G no es 5-resoluble.

Es importante destacar el caso $\pi = p'$. Recordamos que un grupo es *p-nilpotente* si tiene un p'-subgrupo de Hall normal. Así, un grupo *no p-nilpotente minimal* es aquel que todo subgrupo propio es p-nilpotente pero el propio grupo no lo es. Observamos que los grupos no p'-cerrados minimales son los no p-nilpotentes minimales. Estos grupos han sido estudiados por N. Itô en [**26**]. En ese artículo, el autor prueba que un grupo no p-nilpotente minimal es un grupo no nilpotente minimal.

Para probar el Teorema C necesitamos el siguiente resultado de [**32**] el cual depende de la clasificación de los subgrupos de Hall de los grupos simples.

LEMA 3.6. *Sea π un conjunto de primos divisores de $|G|$, donde G es un grupo. Si G tiene τ-subgrupos de Hall nilpotentes para todo $\tau \subset \pi$ con $|\tau| = 2$, entonces G tiene π-subgrupos de Hall nilpotentes.*

Con los resultados mencionados en esta sección junto al Corolario 2.9, podemos proceder con la demostración de los resultados principales de este capítulo.

3.3. Nilpotencia

Vamos a empezar probando el Teorema A, el cual reescribimos a continuación.

TEOREMA 3.7. *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

(i) *G es nilpotente.*

(ii) *Para todos los elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$,*

$$\pi(o(x)o(y)) = \pi(o(xy)).$$

(iii) *Para todos los elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$,*

$$\pi(o(x)o(y)) \subseteq \pi(o(xy)).$$

DEMOSTRACIÓN. Sabemos que si G es nilpotente, para todo $x, y \in G$ de orden coprimo, se tiene que $xy = yx$, y, por tanto, $o(xy) = o(x)o(y)$. En particular, $\pi(o(x)o(y)) = \pi(o(xy))$ para todo $x, y \in G$ con $(o(x), o(y)) = 1$. Así hemos probado que (i) implica (ii) y como es obvio que (ii) implica (iii), vamos a ver que (iii) implica (i).

Supongamos que para todo $x, y \in G$ elementos de orden potencia de primo con $(o(x), o(y)) = 1$ se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. Queremos ver que G es nilpotente. Sea G un contraejemplo minimal. Como la hipótesis se hereda a subgrupos, todo subgrupo de G es nilpotente, es decir, G es un grupo no nilpotente minimal. Por el Lema 3.3, tenemos que $G = PQ$ donde $P \in \mathrm{Syl}_p(G)$ es cíclico y $Q \in \mathrm{Syl}_q(G)$ es normal en G, con $q \neq p$ primos. Como G no es nilpotente, P no es normal y existe un p-elemento $g \in G - P$. Por tanto, existen elementos no triviales $x \in P$, $y \in Q$ tales que $g = xy$. Pero entonces, $\{p, q\} = \pi(o(x)o(y))$ no es subconjunto de $\pi(o(xy)) = \pi(o(g)) = \{p\}$. Esto contradice la hipótesis y, por tanto, obtenemos el resultado. □

A continuación, probamos el Teorema C, el cual reescribimos.

Teorema 3.8. *Sea π un conjunto de primos divisores del orden de un grupo G. Suponemos que para todos los π-elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$, se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. Entonces G tiene π-subgrupos de Hall nilpotentes.*

Demostración. A fin de probar la existencia de π-subgrupos de Hall nilpotentes, podemos suponer por el Lema 3.6, que $\pi = \{p, q\}$ tiene cardinal 2. Además, es suficiente probar que G tiene π-subgrupos de Hall. (Ya que si H es un π-subgrupo de Hall, entonces H satisface la hipótesis (iii) del Teorema A, y, por tanto, es nilpotente.)

Suponemos que G tiene factores de composición de orden divisible por pq. En este caso, el Corolario 2.9 nos asegura que existen $x, y \in G - \{1\}$ con x un p-elemento e y un q-elemento tales que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$. Esto contradice nuestra hipótesis. Por tanto, G no tiene factores de composición de orden divisible por pq. Entonces el Corolario 3.2 implica que G satisface D_π y, por tanto, G tiene π-subgrupos de Hall. El resultado se sigue. □

Como hemos comentado en la introducción de este capítulo, el recíproco de este teorema no es cierto en general, vamos a ver con detalle el ejemplo.

Ejemplo 3.9. Sean $G = \mathrm{PSL}(2, 16)$ y $\pi = \{3, 5\}$. Como $|G| = 2^4 \cdot 3 \cdot 5 \cdot 17$, se tiene que $|G|_\pi = 15$. En G hay elementos de orden 15, por ejemplo

$$g = \begin{pmatrix} 0 & 1 \\ 1 & \delta^7 \end{pmatrix},$$

donde δ es un generador de $\mathbb{F}_{2^4}^\times$. Entonces $\langle g \rangle$ es un π-subgrupo de Hall de G cíclico y, por tanto, nilpotente. Veamos que, en efecto, G contiene elementos x, y de forma que $o(x) = 3$, $o(y) = 5$ y $o(xy) = 17$. Consideramos, por ejemplo, los siguientes elementos:

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & \delta \\ \delta^{-1} & \delta^{10} \end{pmatrix}.$$

Entonces se puede ver fácilmente que $o(x) = 3$, teniendo en cuenta que $1 + 1 = 0$. En efecto,

$$x^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad x^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

De la misma forma se puede ver que $o(y) = 5$ y $o(xy) = 17$.

Como el recíproco es falso en general, podemos estudiar cuáles son los grupos que son contraejemplo. Observamos que por el Corolario 2.9, si un grupo G tiene factores de composición de orden divisible por pq para primos diferentes p y q, entonces existen elementos no triviales $x, y \in G$, con x un p-elemento, y un q-elemento y $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$. Así, cualquier grupo con un factor de composición de orden divisible por pq y con $\{p, q\}$-subgrupos de Hall nilpotentes es un contraejemplo del recíproco del Teorema C.

Además, como una consecuencia inmediata del Corolario 2.9 y el Teorema C, tenemos la siguiente versión más fuerte del Teorema C.

Teorema 3.10. *Sea π un conjunto de primos divisores del orden de un grupo G. Suponemos que para todo par de elementos no triviales $x, y \in G$ que son π-elementos de orden potencia de primo con $(o(x), o(y)) = 1$, se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. Entonces G tiene π-subgrupos de Hall nilpotentes y para todo $p, q \in \pi$ con $p \neq q$, G no tiene factores de composición de orden divisible por pq.*

Uno podría pensar que, quizás, el recíproco de este teorema sí es cierto. Sin embargo también falla, veamos el siguiente ejemplo.

Ejemplo 3.11. Sea $G = \langle x\rangle \mathrm{PSL}(2, 2^5)$ donde x es un automorfismo de tipo cuerpo de $\mathrm{PSL}(2, 2^5)$ de orden 5. Sea $\pi = \{3, 5\}$. Como $|\mathrm{PSL}(2, 2^5)| = 2^5 \cdot 3 \cdot 11 \cdot 31$, se tiene que G es 5-resoluble. Además, $\langle x\rangle$ actúa coprimamente sobre $\mathrm{PSL}(2, 2^5)$. Entonces $\mathrm{PSL}(2, 2^5)$ tiene un 3-subgrupo de Sylow $\langle x\rangle$-invariante. Sea P este subgrupo. Así, el producto $\langle x\rangle P$ es subgrupo de G y es un π-subgrupo de Hall de G. De nuevo, $|G|_\pi = 15$ y deducimos que G tiene $\{3, 5\}$-subgrupos de Hall cíclicos. Consideramos los siguientes generadores del grupo $\mathrm{PSL}(2, 2^5)$:

$$g_1 := \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}, \qquad g_2 := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

donde δ es un generador de $\mathbb{F}_{2^5}^\times$.

Entonces si tomamos, por ejemplo, el elemento $x \in \mathrm{Aut}(\mathrm{PSL}(2, 2^5))$ de orden 5 tal que

$$g_1 \mapsto \begin{pmatrix} \delta^{10} & \delta^{16} \\ \delta^{-4} & \delta^{13} \end{pmatrix}, \qquad g_2 \mapsto \begin{pmatrix} \delta^{2} & \delta^{7} \\ \delta^{15} & \delta^{5} \end{pmatrix},$$

se cumple que existe un elemento $y \in \mathrm{PSL}(2, 2^5)$ de orden 3 tal que el orden de xy es 10.

Sea $y = \begin{pmatrix} \delta^{11} & \delta^{15} \\ \delta^{2} & \delta^{19} \end{pmatrix}$. Se puede ver que $o(y) = 3$ y que $z = xy$ es un elemento de G de orden 10.

En vista de este ejemplo, vamos a ver una variante del Teorema D, la cual prueba que en cualquier contraejemplo del recíproco del Teorema 3.10 aparecen involucrados automorfismos coprimos de grupos simples. De hecho, se sabe que dichos automorfismos están conjugados con automorfismos de tipo cuerpo de los grupos simples de tipo Lie.

TEOREMA 3.12. *Sea π un conjunto de primos divisores de $|G|$, donde G es un grupo. Suponemos que para todo factor de composición no abeliano S de G, se tiene que $\pi(Aut(S)) = \pi(S)$. Las siguientes afirmaciones son equivalentes:*

(i) *Para todos los π-elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$, se cumple que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$.*

(ii) *G tiene π-subgrupos de Hall nilpotentes y para todo $p, q \in \pi$ con $p \neq q$, se tiene que G no tiene factores de composición de orden divisible por pq.*

DEMOSTRACIÓN. Basta probar que (ii) implica (i). Observamos que la hipótesis se hereda a grupos cocientes. Sea G un contraejemplo minimal. Entonces existen $p, q \in \pi$ con $p \neq q$ y $x, y \in G$ tales que $1 \neq x$ es un p-elemento, $1 \neq y$ es un q-elemento y pq no divide a $o(xy)$. Sea N un subgrupo normal minimal de G. Escribimos $\overline{G} = G/N$. Por reducción al absurdo, suponemos que $x, y \notin N$. Entonces $\overline{x}$ e $\overline{y}$ son un p-elemento y un q-elemento no triviales de $\overline{G}$, respectivamente. Por hipótesis, $\overline{G}$ tiene π-subgrupos de Hall nilpotentes. Entonces por la minimalidad de G, tenemos que pq divide a $o(\overline{xy})$. Sin embargo, como $o(\overline{xy})$ divide a $o(xy)$, deducimos que pq divide a $o(xy)$ y llegamos a una contradicción. Sin pérdida de generalidad, podemos suponer que $x \in N$. Además, N es el único subgrupo normal minimal de G. (En caso contrario, existiría un subgrupo normal minimal $M \neq N$ de G. Como antes, podemos suponer que $y \in M$. Como $[N, M] = 1$, se tiene que x e y conmutan y esto contradice el hecho que pq no divide a $o(xy)$.)

Como pq no divide a $|N|$, deducimos que $y \notin N$. Así tenemos que $G = \langle y \rangle N$ (en caso contrario, $\langle y \rangle N$ sería un contraejemplo de orden menor que G). Escribimos $Q = \langle y \rangle$ y notamos que $Q \in \mathrm{Syl}_q(G)$. Ahora, si N es abeliano entonces $G = QN$ es un $\{p, q\}$-grupo. Como G tiene $\{p, q\}$-subgrupos de Hall nilpotentes, deducimos que G es nilpotente. Pero entonces pq divide a $o(xy)$. Llegamos de nuevo a una contradicción.

Podemos suponer que $N = S_1 \times \cdots \times S_n$, donde para todo i, $S_i \cong S$ para algún grupo simple no abeliano S. Como q no divide a $|N|$, sabemos que N tiene un p-subgrupo de Sylow P que es Q-invariante. Por tanto, por hipótesis, QP es un $\{p, q\}$-subgrupo de Hall nilpotente de G. Como N es el único subgrupo normal minimal de G, deducimos que Q permuta transitivamente las n copias de S. En particular, si $n > 1$ entonces Q no centraliza ningún elemento no trivial de S_i para todo i. Pero como Q centraliza P, esto implica que $n = 1$. Así $G = QS$, donde Q actúa no trivialmente sobre S (porque x e y no conmutan). Esto implica que $Q/\mathbf{C}_Q(S)$ es isomorfo a un subgrupo no trivial de $\mathrm{Aut}(S)$. Esto contradice la hipótesis de que $\pi(Aut(S)) = \pi(S)$ y el resultado se sigue. □

Observamos que en el Teorema 3.12 basta suponer que $\pi \cap \pi(\mathrm{Aut}(S)) = \pi \cap \pi(S)$ para obtener la equivalencia. Como consecuencia obtenemos el siguiente corolario.

Corolario 3.13 (J. Sangroniz). *Sea G un grupo con los factores de composición no abelianos de orden múltiplo de un primo $p > 2$. Entonces existen elementos $x, y \in G$ tales que x es un 2-elemento, y un p-elemento y el orden de xy no es múltiplo de $2p$.*

En particular, siguiendo la estructura de la prueba del teorema anterior, vamos a probar el Teorema D, el cual reescribimos.

Teorema 3.14. *Sea π un conjunto de primos divisores de $|G|$, donde G es un grupo π-separable. Las siguientes afirmaciones son equivalentes:*

(i) *Para todos los π-elementos $x, y \in G$ de orden potencia de primo tales que $(o(x), o(y)) = 1$, se cumple que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$.*

(ii) *G tiene π-subgrupos de Hall nilpotentes.*

Demostración. De nuevo basta probar que (ii) implica (i). Observamos que la hipótesis se hereda a grupos cocientes. Sea G un contraejemplo minimal. Entonces existen $p, q \in \pi$ con $p \neq q$ y $x, y \in G$ tales que $1 \neq x$ es un p-elemento, $1 \neq y$ es un q-elemento y pq no divide a $o(xy)$. Sea N un subgrupo normal minimal de G. Escribimos $\overline{G} = G/N$. Por reducción al absurdo, suponemos que $x, y \notin N$. Entonces $\overline{x}$ e $\overline{y}$ son un p-elemento y un q-elemento no triviales de $\overline{G}$, respectivamente. Entonces por la minimalidad de G y por ser $\overline{G}$ π-separable con π-subgrupos de Hall nilpotentes, tenemos que pq divide a $o(\overline{xy})$. Sin embargo, como $o(\overline{xy})$ divide a $o(xy)$, deducimos que pq divide a $o(xy)$ y llegamos a una contradicción. Sin pérdida de generalidad, podemos suponer que $x \in N$. Además, N es el único subgrupo normal minimal de G. (En caso contrario, existiría un subgrupo normal minimal $M \neq N$ de G. Como antes, podemos suponer que $y \in M$. Como $[N, M] = 1$, se tiene que x e y conmutan y esto contradice el hecho que pq no divide a $o(xy)$.)

Ahora, como N es un factor de composición de G y G es π-separable, entonces N es un π-grupo o un π'-grupo. Si N es un π'-grupo, entonces ni p ni q dividen a $|N|$, deducimos que $x, y \notin N$ y esto contradice el hecho de que $x \in N$, con x no trivial. Ahora, si N es un π-grupo, entonces por hipótesis, N está contenido en un π-subgrupo de Hall nilpotente. Luego, N es nilpotente y por, tanto, resoluble. Entonces pq no divide a N. Como pq no divide a $|N|$, deducimos que $y \notin N$. Así tenemos que $G = \langle y \rangle N$

(en caso contrario, $\langle y\rangle N$ sería un contraejemplo de orden menor que G). Escribimos $Q = \langle y\rangle$ y notamos que $Q \in \mathrm{Syl}_q(G)$. Ahora, como N es abeliano entonces $G = QN$ es un $\{p, q\}$-grupo. Como G tiene $\{p, q\}$-subgrupos de Hall nilpotentes, deducimos que G es nilpotente. Pero entonces pq divide a $o(xy)$ y obtenemos la contradicción final. $\square$

Como hemos indicado en la introducción, no es cierto que la condición "para todos los π-elementos $x, y \in G$ con $(o(x), o(y)) = 1$ de orden potencia de primo, $\pi(o(x)o(y)) = \pi(o(xy))$" es equivalente a (i) y (ii) del Teorema D. Vamos a ver en detalle un ejemplo de ello.

Ejemplo 3.15. Tomamos $G = \langle g\rangle E_{5^3}$ el producto semidirecto del 5-grupo extraespecial de orden 5^3 y exponente 5 sobre el que actúa un elemento $g \in \mathrm{Aut}_{\mathbf{Z}(E_{5^3})}(E_{5^3}) = IS$ de orden 6, donde $I = \mathrm{Inn}(E_{5^3}) \cong C_5 \times C_5$ y $S \cong \mathrm{SL}(2, 5)$. Así $g \in \mathrm{SL}(2, 5)$ y $\mathrm{Aut}_{\mathbf{Z}(E_{5^3})}(E_{5^3})$ denota el grupo de automorfismos de E_{5^3} que son la identidad cuando restringimos a $\mathbf{Z}(E_{5^3})$.

Sean, por ejemplo, $g = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ el elemento de orden 6 y

$$\langle g\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\}$$

el subgrupo generado por g. Así, G tiene un π-subgrupo de Hall nilpotente, de hecho cíclico, para $\pi = \{2, 3\}$. Sin embargo, veremos que no cumple que para todos los π-elementos $x, y \in G$ con $(o(x), o(y)) = 1$ de orden potencia de primo, $\pi(o(x)o(y)) = \pi(o(xy))$.

Denotamos por a, b, c los generadores de E_{5^3}, donde $Z = \langle c\rangle$ es el centro de dicho grupo y se tiene que $a^b = ac^4$ y $b^a = bc$. Entonces $E_{5^3}/Z \cong \langle aZ\rangle \times \langle bZ\rangle$ y g actúa de la siguiente forma:

$$\begin{aligned}
(aZ)^g &= g(aZ) = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (ab)Z, \\
(bZ)^g &= g(bZ) = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = a^{-1}Z, \\
c^g &= c.
\end{aligned}$$

Se puede ver que, en general, los elementos de $\langle g\rangle$ actúan de la siguiente forma sobre los elementos a, b, c; donde la siguiente notación significa, por ejemplo en el primer caso, que $a^g = ab$, $b^g = a^4$ y $c^g = c$.

$$\begin{aligned}
g &: \ (a, b, c) \mapsto (ab, a^4, c) \\
g^2 &: \ (a, b, c) \mapsto (bc^4, a^4b^4c, c) \\
g^3 &: \ (a, b, c) \mapsto (a^4c^4, b^4c, c) \\
g^4 &: \ (a, b, c) \mapsto (a^4b^4, ac, c) \\
g^5 &: \ (a, b, c) \mapsto (b^4, abc, c)
\end{aligned}$$

Por tanto, si tomamos, por ejemplo, los siguientes elementos:

$$\begin{aligned} x &= (g^3, b^2c^{-1}), \\ y &= (g^4, b^3), \\ z := xy &= (g, a^2b^3c), \end{aligned}$$

entonces se cumple que $o(x) = 2$, $o(y) = 3$ y $o(xy) = 30$. De esta forma se tiene que $\{2, 3, 5\} = \pi(o(xy))$ no está incluido en $\{2, 3\} = \pi(o(x)o(y))$.

Veamos, por ejemplo, que $o(x) = 2$:

$$\begin{aligned} x^2 &= (g^3, b^2c^{-1})(g^3, b^2c^{-1}) = (g^6, (b^2c^{-1})^{g^3}b^2c^{-1}) = \\ &= (1, (b^4c)^2c^{-1}b^2c^{-1}) = (1, b^3cb^2c^{-1}) = (1, 1). \end{aligned}$$

3.4. Existencia de subgrupos de Hall normales

En esta sección, dado un conjunto de primos π que dividen al orden de un grupo, obtenemos una caracterización de la existencia de un π-subgrupo de Hall normal, en términos de los conjuntos de primos divisores de los órdenes de ciertos productos de elementos (Teorema E). En primer lugar, vamos a ver un par de resultados previos, los cuales se deben a M. D. Pérez-Ramos. Empezamos con la siguiente observación.

Lema 3.16 (Pérez-Ramos). *Sean G un grupo y π un conjunto de primos. Las siguientes afirmaciones son equivalentes:*

(i) *G no tiene factores de composición de orden divisible por pq para todo par de primos $p \in \pi$, $q \in \pi'$.*
(ii) *G es π-separable.*

Teorema 3.17 (Pérez-Ramos). *Sean G un grupo y π un conjunto de primos. Supongamos que para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$. Entonces G es π-separable.*

Demostración. Por el lema anterior, es suficiente probar que G no tiene factores de composición de orden divisible por pq para todo par de primos $p \in \pi$ y $q \in \pi'$. Por reducción al absurdo, supongamos que existen primos $p \in \pi$, $q \in \pi'$ tales que G tiene algún factor de composición de orden divisible por pq. Por el Corolario 2.9, existen elementos $x, y \in G$ con $1 \neq x$ un p-elemento, $1 \neq y$ un q-elemento tales que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \emptyset$, pero por hipótesis $\pi(o(y)) \subseteq \pi(o(xy))$, lo cual es una contradicción. □

A continuación, probamos el Teorema E, el cual reescribimos. La demostración que presentamos se debe a Pérez-Ramos y simplifica nuestra prueba original.

Teorema 3.18. *Sea G un grupo y sea $\pi \subseteq \pi(G)$. Entonces las siguientes afirmaciones son equivalentes:*

(i) *Para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.*
(ii) *G tiene un π-subgrupo de Hall normal.*

Demostración. Suponemos primero que G tiene un π-subgrupo de Hall normal. Sea H este subgrupo. Sean $x, y \in G$ tales que x es un p-elemento con $p \in \pi$ e y es un q-elemento con $q \in \pi'$. Como H es normal en G se tiene que $x \in H$ y que $xyH = yxH = yH$. Por tanto, se tiene que $H = (xyH)^{o(xy)} = (yH)^{o(xy)}$. Deducimos que $o(yH)$ divide a $o(xy)$ y como $o(yH) = o(y)$, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.

Ahora, vamos a ver el recíproco. Sea G un contraejemplo minimal, es decir, G es un grupo de orden minimal satisfaciendo que para todo par de elementos $x, y \in G$ con x un π-elemento y con y un π'-elemento, ambos de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$ y, además, G no tiene un π-subgrupo de Hall normal.

Por el teorema anterior, deducimos que G es π-separable. Ahora, por ser G un contraejemplo minimal, G es no π-cerrado minimal. Por la Proposición 3.5, $\pi(G) = \pi \cup \{q\}$ con $q \in \pi(G) - \pi$. En este caso se tiene que π-cerrado es equivalente a q-nilpotente y, por ello, G es no q-nilpotente minimal. Por el resultado de Itô, G es no nilpotente minimal, luego $\pi(G) = \{p, q\}$ y $G = PQ$ con P un p-subgrupo de Sylow no normal y Q un q-subgrupo de Sylow no trivial, por el Lema 3.3. En particular, existe un p-elemento $g \in G - P$ no trivial y existen elementos no triviales $x \in P$, $y \in Q$ tales que $g = xy$. Luego $\{q\} = \pi(o(y)) \nsubseteq \pi(o(xy)) = \pi(o(g)) = \{p\}$, con lo que obtenemos una contradicción. □

Por último, como aplicación del Teorema 3.18, obtenemos la siguiente caracterización de la existencia de un π-subgrupo de Hall como factor directo.

Teorema 3.19. *Sea π un conjunto de primos divisores del orden de un grupo G. Entonces las siguientes afirmaciones son equivalentes:*

(i) *Para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, $\pi(o(x)o(y)) \subseteq \pi(o(xy))$.*
(ii) *$G = H_\pi \times H_{\pi'}$, donde H_π es un π-subgrupo de Hall de G y $H_{\pi'}$ es un π'-subgrupo de Hall de G.*

Demostración. Suponemos que para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, se cumple que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. En particular, para todo π-elemento x de G y todo π'-elemento y de G, ambos de orden potencia de primo, se cumple tanto que $\pi(o(x)) \subseteq \pi(o(xy))$ como que $\pi(o(y)) \subseteq \pi(o(xy))$. Aplicando el Teorema 3.18, tenemos que G tiene un π-subgrupo de Hall normal y un π'-subgrupo de Hall normal y se deduce (ii). El recíproco es inmediato. □

Nótese que el teorema anterior puede probarse también usando el Teorema C y el Ejemplo 1 de [**15**] (para los conjuntos de primos π y π').

3.5. Más resultados

Comenzamos esta sección con varias demostraciones alternativas a las vistas en las secciones anteriores. En primer lugar, empezamos con una prueba del Teorema E en el caso que $\pi = p'$, ya que en ese caso el grupo es resoluble y la prueba se simplifica. De hecho, la demostración que ahora presentamos no necesita la Clasificación de los Grupos Simples Finitos.

Teorema 3.20. *Sea G un grupo y sea $p \in \pi(G)$. Entonces las siguientes afirmaciones son equivalentes:*

(i) *Para todo p'-elemento x de G de orden potencia de primo y todo p-elemento y de G, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.*

(ii) *G es p-nilpotente.*

Demostración. Basta probar que (i) implica (ii). Suponemos que G es un contraejemplo minimal, es decir, un grupo de orden mínimo tal que no es p-nilpotente y cumple que para todo p'-elemento x de G de orden potencia de primo y todo p-elemento no trivial y de G, se tiene que p divide a $o(xy)$. Por la elección de G, deducimos que todo subgrupo propio de G es p-nilpotente pero G no lo es, es decir, todo subgrupo propio de G tiene un p'-subgrupo de Hall normal. Entonces G es un grupo no p-nilpotente minimal, en particular, por el Teorema de Itô, G es no nilpotente minimal. Por tanto, por el Lema 3.3 tenemos que $G = QP$ donde $P \in \mathrm{Syl}_p(G)$ es normal en G y $Q \in \mathrm{Syl}_q(G)$ es cíclico, con $q \neq p$ primo. Sea $Q = \langle x \rangle$, donde x es un q-elemento. Entonces $G = \langle x \rangle P$. Como G no es nilpotente, deducimos que $[x, P] \neq 1$. Se sigue que existe algún elemento $z \in P$ tal que $[x, z] \neq 1$. Sea $y = [x, z] \in P$ un p-elemento. Entonces $x^z = x[x, z] = xy$ es un q-elemento. Sin embargo, por hipótesis, $o(xy)$ es divisible por p, lo cual es una contradicción. Por tanto, G es p-nilpotente, como queríamos demostrar. □

En segundo lugar, queremos mostrar la prueba original del Teorema E para el caso $\pi = \{p\}$. Este resultado es el Teorema C de [**33**].

Teorema 3.21. *Sean G un grupo y p un primo. Entonces G tiene un p-subgrupo de Sylow normal si y solo si para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.*

Demostración. Basta ver que G tiene un p-subgrupo de Sylow normal si para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$. Sea G un contraejemplo minimal. Como la hipótesis se hereda a subgrupos, todo subgrupo propio de G tiene un p-subgrupo de Sylow normal pero G no lo tiene. Por tanto, G es un grupo no p-cerrado minimal.

Suponemos que G contiene un factor de composición de orden divisible por pq, para algún primo $q \neq p$. Por tanto, por el Corolario 2.9, existen elementos no triviales $x, y \in G$ con x un p-elemento, y un q-elemento tales que $\pi(o(x)o(y)) \cap \pi(o(xy)) = \varnothing$. Esto es una contradicción.

Suponemos que G es un grupo sin factores de composición de orden divisible por pq, para todo primo $q \neq p$. Por tanto, G es p-resoluble. Por el Lema 3.4, se tiene que $|\pi(G)| = 2$. Sea $\pi(G) = \{p, q\}$. Tenemos que $G = PQ$, donde $P \in \mathrm{Syl}_p(G)$ y $Q \in \mathrm{Syl}_q(G)$. Ahora, como P no es normal, existe un p-elemento $g \in G - P$. Por tanto, existen elementos no triviales $x \in P$, $y \in Q$ tales que $g = xy$. Pero entonces $\{q\} = \pi(o(y))$ no es un subconjunto de $\pi(o(xy)) = \pi(o(g)) = \{p\}$. Esto supone la contradicción final. □

Ahora, vamos a ver la prueba original del Teorema 3.19 en el caso $\pi = \{p\}$ donde se caracteriza la existencia de un subgrupo de Sylow como factor directo (es el Teorema F de [**33**]). Previamente, vamos a ver un lema que puede tener interés por sí mismo.

Lema 3.22. *Sean G un grupo y p un primo. Suponemos que G tiene $\{p, q\}$-subgrupos de Hall nilpotentes para todo primo q. Entonces $G = P \times H$ donde $P \in \mathrm{Syl}_p(G)$ y H es un p'-subgrupo de Hall de G.*

Demostración. Sea $P \in \mathrm{Syl}_p(G)$. Por hipótesis, $N_G(P)$ contiene un q-subgrupo de Sylow de G para todo primo q. Por tanto, $N_G(P)$ tiene orden un múltiplo del orden de G y deducimos que $N_G(P) = G$. Esto implica que P es normal en G.

Por el Teorema de Schur-Zassenhaus, tenemos que $G = HP$, donde H es un p'-subgrupo de Hall de G. Sean $\{p, q_1, \dots, q_n\}$ el conjunto de primos divisores de $|G|$ y $Q_i \in \mathrm{Syl}_{q_i}(H)$ para todo i. Observamos que los subgrupos Q_i son también subgrupos de Sylow de G y que $H = \langle Q_1, \dots, Q_n\rangle$. También podemos observar que Q_iP es un $\{p, q_i\}$-subgrupo de Hall de G y además nilpotente (porque todos los $\{p, q_i\}$-subgrupos de Hall son conjugados, por [**42**]). Por tanto, P centraliza Q_i para todo i y el resultado se sigue. □

Observamos que este lema es un caso particular del resultado [**15**, Ejemplo 1] para los conjuntos de primos $\{p\}$ y p'. Ahora, procedemos con la prueba del teorema mencionado arriba.

Teorema 3.23. *Sea G un grupo y sea p un primo. Las siguientes afirmaciones son equivalentes:*

(i) *Para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo, se cumple que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$.*
(ii) *$G = P \times H$, donde $P \in \mathrm{Syl}_p(G)$ y H es un p'-subgrupo de Hall de G.*

Demostración. Basta ver que (i) implica (ii). Suponemos que para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo, se tiene que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$. Por el Teorema C, sabemos que G tiene $\{p, q\}$-subgrupos de Hall nilpotentes para todo primo q. El resultado se sigue del Lema 3.22. □

Concluimos esta primera parte de la sección con una prueba alternativa a la Proposición 3.5. Este resultado nos da información sobre el conjunto de primos que divide al orden de un grupo π-separable no π-cerrado minimal. En primer lugar, enunciamos el siguiente lema elemental que es bien conocido.

LEMA 3.24. *Sea G un grupo. Se tiene que:*

(i) *Si N es un subgrupo normal de un grupo π-cerrado G, entonces G/N es π-cerrado.*
(ii) *Si N, M son subgrupos normales de G tales que G/N y G/M son π-cerrados, entonces $G/N \cap M$ es π-cerrado.*
(iii) *Si $G/\Phi(G)$ es π-cerrado, entonces G es π-cerrado.*

Una forma alternativa de enunciar el lema anterior es decir que la clase de los grupos π-cerrados es una formación saturada. Ahora, vemos dicha prueba alternativa omitiendo algunos detalles.

PROPOSICIÓN 3.25. *Sea G un grupo π-separable no π-cerrado minimal con $\pi \subseteq \pi(G)$ no vacío. Entonces $\pi(G) = \pi \cup \{q\}$, con $q \in \pi(G) - \pi$.*

DEMOSTRACIÓN. (Pérez-Ramos) Suponemos que G es un contraejemplo minimal. En primer lugar, como $\pi(G) = \pi(G/\Phi(G))$ y G es contraejemplo minimal, usando el lema anterior, obtenemos que $\Phi(G) = 1$.

Ahora, sea N un subgrupo normal minimal de G. Como $\Phi(G) = 1$, existe $U < G$ tal que $G = NU$. Como G es no π-cerrado minimal, se tiene que U es π-cerrado. Por tanto, $G/N \cong U/U \cap N$ es π-cerrado. Además, deducimos por el lema anterior que G tiene un único subgrupo normal minimal N.

Veamos que $N < G$ y es π'-grupo. Por ser N minimal normal, tenemos que N es característicamente simple, N es p-grupo para algún primo p o producto directo de grupos simples no abelianos isomorfos, y como es π-separable, N debe ser π-grupo o π'-grupo. En particular, $N < G$. Además, como hemos visto que G/N es π-cerrado, si N fuese π-grupo, tendríamos que G es π-cerrado, lo cual es una contradicción. Luego N es π'-grupo.

Supongamos ahora que $H/N = \mathbf{O}_\pi(G/N) < G/N$. Por el Teorema de Schur-Zassenhaus y por la hipótesis, tenemos que $H = NK$ es π-cerrado donde $K = \mathbf{O}_\pi(H)$ es π-subgrupo de Hall de H. Entonces, deducimos que $[N, K] \leq N \cap K = 1$, es decir, $K \leq \mathbf{C}_G(N) \leq N$. Esto implica que $K = 1$, $H = N$ y G es un π'-grupo, lo que nos lleva de nuevo a una contradicción. Luego $G/N = \mathbf{O}_\pi(G/N)$.

Finalmente, vamos a ver que $|\pi(N)| = 1$. Para ello, suponemos que $|\pi(N)| \geq 2$. Sea $p \in \pi(N)$. Por el Teorema de Schur-Zassenhaus, $G = NL$ donde L es un π-subgrupo de Hall de G. Como N es un π'-subgrupo normal de G, existe un p-subgrupo de Sylow P de N que es L-invariante. Entonces $PL < G$, y por hipótesis, PL es π-cerrado. Luego, como antes, $L \leq \mathbf{C}_G(P)$. En consecuencia, $L \leq \mathbf{C}_G(N) \leq N$, esto implica que $L = 1$ y $G = N$, lo cual es una contradicción. Por tanto, $|\pi(N)| = 1$, luego $\pi(G) = \pi \cup \{q\}$ con $q \in \pi(G) - \pi$. □

El resto de la sección está destinado a una serie de cuestiones relacionadas con las secciones anteriores.

En vista del Teorema C, nos interesamos ahora en caracterizar los grupos G con la propiedad de que para algún π conjunto de primos divisores de $|G|$ y para todos los π-elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$, se cumple que $\pi(o(xy)) \subseteq \pi(o(x)o(y))$. Sin embargo, esta pregunta no es sencilla, por ello, nos centramos primero en estudiar cómo son los grupos que cumplen la siguiente hipótesis, que es su versión global.

Hipótesis 1. Sea G un grupo tal que $\pi(o(xy)) \subseteq \pi(o(x)o(y))$ para todos los elementos $x, y \in G$ (de orden potencia de primo) con $(o(x), o(y)) = 1$.

Cuestión 3. ¿Cuáles son los grupos G que satisfacen la Hipótesis 1?

Usando GAP [**12**], se puede ver que la mayoría de los grupos resolubles (hasta orden 2000) cumplen la Hipótesis 1. Comenzamos viendo alguna condición necesaria o suficiente para que un grupo cumpla dicha hipótesis.

Por ejemplo, vamos a ver que si $PQ = QP$ para todo par de subgrupos de Sylow de G de órdenes coprimos, entonces G cumple la Hipótesis 1. Esta propiedad ya ha sido estudiada. A los subgrupos H que permutan con todos los subgrupos de Sylow de orden coprimo con H se les denomina *S-semipermutables*. Existen varios artículos que estudian propiedades acerca de la S-semipermutabilidad. Por ejemplo, Isaacs en [**25**] demuestra que si un p-subgrupo de Sylow de un grupo G es S-semipermutable, entonces G es p-resoluble.

Teorema 3.26. *Sea G un grupo.*

(i) *(Sangroniz) Si G es metabeliano entonces G cumple la Hipótesis 1.*
(ii) *Si G es tal que todo subgrupo de Sylow es S-semipermutable, entonces G cumple la Hipótesis 1.*
(iii) *Si G cumple la Hipótesis 1 entonces G es resoluble.*

Los recíprocos son falsos.

Demostración. En primer lugar, probamos (i). Sea G un contraejemplo minimal. Entonces existen elementos $x, y \in G$ tales que $(o(x), o(y)) = 1$ y $\pi(o(xy)) \nsubseteq \pi(o(x)o(y))$. Llamamos $\pi = \pi(o(x)o(y))$. Como G es contraejemplo minimal, $G = \langle x, y \rangle$. Además, como G' es abeliano, $G' = A \times B$ donde A es un π-subgrupo de Hall de G' y B un π'-subgrupo de Hall de G'. Como G/A es también contraejemplo, deducimos que $A = 1$. Llamamos $\overline{G} = G/G'$. Como $(o(\overline{x}), o(\overline{y})) = 1$ y G' es abeliano, se tiene que $\overline{G} = \langle \overline{x}, \overline{y} \rangle = \langle \overline{xy} \rangle$ es un grupo cíclico de orden $o(x)o(y)$. Así, $G = CG'$ es el producto semidirecto de un grupo cíclico C de orden $o(x)o(y)$ y el π'-subgrupo de Hall G'.

Como C es un π-subgrupo de Hall, podemos suponer que $x \in C$. Además, como y es un π-elemento, se tiene que $y = {y_0}^n$ con $y_0 \in C$, $n \in G'$. Entonces $xy = xy_0^n = xy_0[y_0, n] = xy_0 m$ con $m \in G'$. Por otro lado, como C y G' son abelianos, $G' = [G, G] = [CG', CG'] = [C, G'] = \{[xy_0, g] \mid g \in G'\}$. Luego podemos escribir $xy = xy_0[xy_0, g] = (xy_0)^g$ con $x, y_0 \in C$ y $g \in G$. Como

C es cíclico y los elementos xy y xy_0 son conjugados en G, obtenemos que $\pi(o(xy)) = \pi(o(xy_0)) = \pi(o(x)o(y_0)) = \pi(o(x)o(y))$, lo cual contradice el hecho que G es contraejemplo y hemos completado la prueba de (i).

A continuación, vamos a ver (ii). Sea G un grupo tal que todo subgrupo de Sylow es S-semipermutable. Sean $x, y \in G$ tales que $(o(x), o(y)) = 1$. Entonces podemos escribir $x = x_{p_1} \cdots x_{p_r}$ e $y = y_{q_1} \cdots y_{q_s}$, donde los x_i conmutan entre ellos, los y_j también y $\{p_1, \ldots, p_r\} = \pi(o(x))$ y $\{q_1, \ldots, q_s\} = \pi(o(y))$. Por hipótesis, tenemos que $P_iQ_j = Q_jP_i$ para todo $P_i \in \mathrm{Syl}_{p_i}(G)$, para todo $Q_j \in \mathrm{Syl}_{q_j}(G)$ y para todo $1 \leq i \leq r$ y $1 \leq j \leq s$. Por inducción, tenemos que $P_1 \cdots P_rQ_1 \cdots Q_s = Q_1 \cdots Q_sP_1 \cdots P_r$ y, por tanto, $P_1 \cdots P_rQ_1 \cdots Q_s$ es un $\{p_1, \ldots, p_r, q_1 \ldots, q_s\}$-subgrupo de Hall. Ahora, como $x_{p_i} \in P_i$ para algún $P_i \in \mathrm{Syl}_{p_i}(G)$ e $y_{q_j} \in Q_j$ para algún $Q_j \in \mathrm{Syl}_{q_j}(G)$, se tiene que $xy \in P_1 \cdots P_rQ_1 \cdots Q_s$. Por tanto, $\pi(o(xy)) \subseteq \pi(o(x)o(y))$ y se cumple la Hipótesis 1.

Por último, por el Teorema de Thompson (o el Teorema de Guralnick-Tiep, para los elementos de orden potencia de primo), tenemos que los grupos que cumplen la Hipótesis 1 son resolubles.

Ahora, vamos a ver que los recíprocos son falsos. Comenzamos viendo un ejemplo de un grupo que cumple la Hipótesis 1 pero no es metabeliano. Basta tomar el grupo $G = \mathrm{SL}(2, 3)$. Observamos claramente que este grupo cumple la Hipótesis 1 pero no es metabeliano (ya que $G' = Q_8$, el grupo cuaternio).

También hay grupos que cumplen la Hipótesis 1 pero no cumplen que todo subgrupo de Sylow es S-semipermutable. Veamos un ejemplo.

Consideramos de nuevo $G = \langle a, b \mid a^6 = 1 = b^7, b^a = b^5 \rangle$ el grupo de Frobenius de orden 42 del Ejemplo 2.15. Sea N el subgrupo normal de orden 7 de G. Entonces, como $G/N \cong C_6$, deducimos que para todo $x, y \in G$ tales que $o(x) = 2$, $o(y) = 3$, se tiene que $o(xy) = 6$. En efecto, se tiene que $o(xN) = 2$, $o(yN) = 3$ y $o(xNyN) = o(xyN) = 6$. Como $o(xyN)$ divide a $o(xy)$, deducimos que $o(xy) = 6$. Por tanto, cumple la Hipótesis 1 y, sin embargo, no es cierto que cualquier 2-subgrupo de Sylow conmuta con cualquier 3-subgrupo de Sylow. Veámoslo. Consideramos, por ejemplo, los siguientes subgrupos de Sylow. Sea $P = \langle (a^3)^g \rangle = \langle a^3b^2 \rangle \in \mathrm{Syl}_2(G)$, donde $g = a^3b$ y $Q = \langle a^4 \rangle \in \mathrm{Syl}_3(G)$. Entonces P y Q no conmutan, ya que

$$PQ = \left\{1, a^4, a^2, a^3b^2, ab^4, a^{-1}b\right\} \neq \left\{1, a^4, a^2, a^3b^2, ab^2, a^{-1}b^2\right\} = QP.$$

Concluimos con un ejemplo de un grupo resoluble que no cumple la Hipótesis 1.

Sea G el producto semidirecto de S_3 (el grupo simétrico de grado 3) actuando fielmente sobre $C_5 \times C_5$. Vamos a encontrar elementos $x, y \in G$ con $o(x) = 2, o(y) = 3$ y $o(xy) = 10$. Así, tenemos que G es un grupo resoluble y, sin embargo, $\pi(o(xy)) = \{2, 5\} \nsubseteq \pi(o(x)o(y)) = \{2, 3\}$.

Podemos escribir $G = \langle a, b, c, d\rangle$, de forma que $o(a) = 2$, $o(b) = 3$, $o(c) = o(d) = 5$ y se cumplen las siguientes relaciones:

$$b^a = b^{-1},\ c^a = c,\ d^a = (dc)^{-1},\ c^b = cd^3,\ d^b = (d^2c)^{-1}.$$

Entonces tomamos $x = a$, $y = bc$. Se puede comprobar que $z = xy = abc$ tiene orden 10. $\square$

Este resultado motiva la siguiente cuestión, que será estudiada en el Apéndice C.

Cuestión 4. ¿Cuáles son los grupos que satisfacen la propiedad de que todo subgrupo de Sylow es S-semipermutable?

Ahora, nos preguntamos qué sucede con los grupos de Frobenius o los grupos superresolubles.

En primer lugar, observamos que es equivalente ver si la Hipótesis 1 se cumple para un grupo de Frobenius que verlo para un complemento de Frobenius. Sea G un grupo de Frobenius con núcleo N y complemento H. Basta ver que si la hipótesis es cierta para H entonces lo es para G. Sean $x, y \in G$ tales que $(o(x), o(y)) = 1$. Si $x, y \in N$ entonces como los núcleos de Frobenius son nilpotentes, se tiene que $\pi(o(xy)) \subseteq \pi(o(x)o(y))$. Ahora, si $x \in H$ e $y \in N$, se deduce que xy es conjugado a x, luego $o(xy) = o(x)$ lo que implica que $\pi(o(xy)) \subseteq \pi(o(x)o(y))$. Por último, si $x \in H$ e $y \notin N$, tenemos que $y = {y_0}^n$, con $y_0 \in H$, $n \in N$ y se deduce que xy es un conjugado de $xy_0 \in H$. Por tanto, es equivalente ver que $\pi(o(xy)) \subseteq \pi(o(x)o(y))$ para todo $x, y \in G$ que ver que $\pi(o(xy_0)) \subseteq \pi(o(x)o(y_0))$ con $x, y_0 \in H$.

Además, como los complementos de Frobenius de orden impar son metacíclicos y la cuestión sí es cierta para grupos metabelianos, en particular para metacíclicos, deducimos que la Hipótesis 1 es cierta para los grupos de Frobenius de orden impar.

Ahora, para los grupos superresolubles, como G' es nilpotente, de forma análoga al Teorema 3.26 (i) se puede reducir la cuestión al caso en que G' es un π'-subgrupo de Hall. Sin embargo, no se puede asegurar que $[C, G'] = \{[xy_0, g] \mid g \in G'\}$ y por tanto no podemos completar la prueba de la misma manera.

Dada la abundancia de los grupos que cumplen la Hipótesis 1, podría ser más fácil clasificar los grupos minimales que no la cumplen. Sin embargo, tampoco es sencillo. En el Apéndice B podemos encontrar una lista con los grupos hasta orden 2000 tales que no cumplen la Hipótesis 1 pero todos sus subgrupos propios, cocientes y subcocientes sí la cumplen. Salvo el grupo del Ejemplo 3.15 y el grupo de orden 1500 que podemos ver en la lista, todos los grupos minimales en el sentido mencionado son tales que G o $G/Z(G)$ es 2-Frobenius.

En vista de los resultados de este capítulo, es natural preguntarse si se pueden debilitar las hipótesis aún más, por ejemplo sin exigir que se cumplan para todos los elementos de orden potencia de primo. Pensamos que la respuesta a la siguiente pregunta puede ser afirmativa.

Cuestión 5. Sean G un grupo y π un conjunto de primos divisores de $|G|$. Sea P_i un p_i-subgrupo de Sylow para cada primo p_i de π. Supongamos que $\pi(o(x)o(y)) \subseteq \pi(o(xy))$ para todo $x \in P_i$, $y \in P_j$, para todo $i \neq j$. ¿Es cierto que G tiene un π-Hall nilpotente?

Una respuesta afirmativa a esta pregunta en el caso $\pi = \pi(G)$ nos daría versiones más fuertes del Teorema A y del Corolario B. También se podría pensar que con la hipótesis de la Cuestión 5, $[P_i, P_j] = 1$ para cualesquiera $i \neq j$. Sin embargo, esto es falso.

Ejemplo 3.27. Consideramos de nuevo $G = \langle a, b \mid a^6 = 1 = b^7, b^a = b^5 \rangle$ el grupo de Frobenius de orden 42. Hemos visto en la prueba del Teorema 3.26 que este grupo cumple que $o(x)o(y) = o(xy)$ para todo $x, y \in G$ tales que x es un 3-elemento e y un 2-elemento. En particular, $\pi(o(x)o(y)) \subseteq \pi(o(xy))$ para todo $x \in P$ y para todo $y \in Q$ donde $P = \langle a^4 \rangle \in \mathrm{Syl}_3(G)$ y $Q = \langle a^3 b \rangle \in \mathrm{Syl}_2(G)$. Sin embargo, como vimos en el Ejemplo 2.15, los elementos $g = a^4$ y $h = a^3 b$ no conmutan, luego $[g, h] \neq 1$. Deducimos que $[P, Q] \neq 1$.

Capítulo 4

Partiendo de un elemento

4.1. Introducción

En este capítulo obtenemos versiones elemento a elemento de resultados del capítulo anterior. Recordamos que el Corolario 3.21 dice que dado un grupo G y un primo p, G tiene un p-subgrupo de Sylow normal si y solo si para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$. Ahora, partimos de que se cumple esa condición para un p-elemento x fijo, y queremos averiguar si x pertenece a algún p-subgrupo normal. Hemos obtenido el siguiente resultado.

Teorema F. *Sean G un grupo y p un primo. Sea $x \in G$ un p-elemento. Suponemos que G es un grupo sin factores de composición de tipo Lie en característica p. Entonces $x \in \mathbf{O}_p(G)$ si y solo si para todo $q \neq p$ y para todo q-elemento no trivial $y \in G$, se tiene que $\pi(o(y)) \subseteq \pi(o(xy))$.*

Este teorema, como se puede deducir por la hipótesis sobre sus factores de composición, depende del Teorema 2.12. Concretamente, en este capítulo vamos a ver la versión π de este resultado.

Teorema G. *Sea G un grupo. Suponemos que π es un conjunto de primos. Sea $x \in G$ un π-elemento. Suponemos que G es un grupo cuyos factores de composición son cíclicos, alternados, espóradicos o grupos simples de tipo Lie en característica coprima con $o(x)$. Entonces $x \in \mathbf{O}_\pi(G)$ si y solo si para todo $q \in \pi'$ y para todo q-elemento no trivial $y \in G$, se tiene que q divide a $o(xy)$.*

Aplicando el Teorema G a todo π-elemento de orden potencia de primo, conseguimos la caracterización de los grupos con un π-subgrupo de Hall normal en términos de órdenes de productos, es decir, el Teorema E obtenido en el capítulo anterior. Luego los resultados de este capítulo, una vez se consiga completar la demostración de la Conjetura 2.11, serán generalizaciones de los del capítulo anterior.

En particular, si $\pi = p'$, tenemos:

Teorema H. *Sean G un grupo y p un primo. Sea $x \in G$ un p'-elemento. Suponemos que G es un grupo cuyos factores de composición son cíclicos, alternados, espóradicos o grupos simples de tipo Lie en característica p. Entonces se tiene que $x \in \mathbf{O}_{p'}(G)$ si y solo si para todo p-elemento no trivial $y \in G$, p divide a $o(xy)$.*

Nos parece conveniente destacar que en el Teorema H, por ejemplo, no basta con que la propiedad se cumpla para todos los p-elementos no triviales y de un p-subgrupo de Sylow en concreto, sino que es necesario que sea cierto para todos los p-elementos no triviales y de G. Veamos un ejemplo de ello.

Ejemplo 4.1. Sea $G = \mathrm{PSL}(2, 16)$ y en este grupo consideramos los elementos:

$$g = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad x = \begin{pmatrix} 0 & \delta^5 \\ \delta^{10} & \delta^3 \end{pmatrix},$$

donde δ es un generador de $\mathbb{F}_{2^4}^{\times}$. Es rutinario comprobar que $o(g) = 3$ y $o(x) = 17$. Sea $P = \langle g \rangle$ un 3-subgrupo de Sylow. Se tiene que 3 divide a $o(xy)$ para todo $1 \neq y \in P$, pero $\mathbf{O}_{3'}(G) = 1$.

Los resultados enunciados forman parte de la Sección 2 de [**3**].

4.2. Demostraciones

Comenzamos con un sencillo lema.

Lema 4.2. *Sea L un subgrupo normal de un grupo G. Sea π un conjunto de primos y sea $x \in G$ un π-elemento. Si $[x, L] \neq 1$, entonces existe un π-elemento en $xL - \{x\}$.*

Demostración. Por hipótesis, existe algún $y \in L$ tal que $[x, y] \neq 1$. Entonces $x^y = x[x, y] \in xL - \{x\}$ es un π-elemento. $\square$

A continuación, probamos un resultado del cual obtendremos los teoremas de la introducción.

Teorema 4.3. *Sea G un grupo y suponemos que π es un subconjunto propio no vacío de $\pi(G)$. Suponemos que la Conjetura 2.11 es cierta para todos los π-elementos de todos los grupos cuyo socle es un factor de composición de G. Sea $x \in G$ un π-elemento. Entonces para todo $q \in \pi'$ y todo q-elemento no trivial $y \in G$, se tiene que q divide a $o(xy)$ si y solo si $x \in \mathbf{O}_\pi(G)$.*

Demostración. Empezamos suponiendo que $x \in \mathbf{O}_\pi(G)$. Entonces para todo $q \in \pi'$ y para todo q-elemento no trivial $y \in G$, se cumple que $xy \in \mathbf{O}_\pi(G)\langle y \rangle$. Este subgrupo contiene un π-subgrupo de Hall normal. Por tanto, si q no divide a $o(xy)$, entonces xy es un π-elemento tal que $xy \in \mathbf{O}_\pi(G)$. Esto implica que $y \in \mathbf{O}_\pi(G)$, lo cual contradice el hecho de que y es un q-elemento no trivial, con $q \in \pi'$.

Suponemos ahora que para todo $q \in \pi'$ y todo q-elemento no trivial $y \in G$, se tiene que q divide a $o(xy)$. Queremos probar que $x \in \mathbf{O}_\pi(G)$. Sea G un contraejemplo minimal. Podemos suponer que π es un subconjunto propio no vacío de $\pi(G)$.

Paso 1: Sea $L = \mathbf{O}_\pi(G)$. Afirmamos que $L = 1$.

Por reducción al absurdo, supongamos que $L > 1$. Suponemos que existe $q \in \pi'$ y un q-elemento no trivial $yL \in G/L$ de modo que q no divide a $o(xyL)$. Como se tiene que $yL = y_qL$, donde y_q es la q-parte de y, entonces podemos suponer que $y \in G$ es un q-elemento. Entonces $L\langle xy\rangle$ es un q'-grupo, lo cual implica que q no divide a $o(xy)$ y esto contradice nuestra hipótesis. Por tanto, la hipótesis se cumple para G/L y deducimos que $xL \in \mathbf{O}_\pi(G/L) = L/L$. Se sigue que $x \in L$, lo cual es una contradicción. Por tanto, $\mathbf{O}_\pi(G) = 1$.

Paso 2: Sean $r \in \pi'$ y $R = \mathbf{O}_r(G)$. Afirmamos que $R = 1$.

Suponemos que $R > 1$. Queremos ver que la hipótesis se cumple para $\overline{G} = G/R$. Tomamos $q \in \pi'$ y un q-elemento no trivial $\overline{y} \in \overline{G}$. Podemos suponer que $y \in G$ es un q-elemento no trivial.

Consideramos, en primer lugar, que $q = r$. Suponemos contrariamente que q no divide a $o(\overline{xy})$. Por tanto, $\overline{xy}$ es un q'-elemento y deducimos que existe un elemento $z \in R$ tal que $xyz = t$ para algún q'-elemento $t \in G$. Observamos que yz es un q-elemento. Así, tenemos que q no divide a $o(xyz)$, lo cual, por hipótesis, implica que $yz = 1$. Deducimos que $y \in R$, esto es, $\overline{y} = \overline{1}$, lo cual contradice el hecho que $\overline{y}$ es no trivial. Luego, podemos suponer que $q \neq r$. Suponemos, de nuevo, que q no divide a $o(\overline{xy})$. Como R es un r-grupo, se tiene que q tampoco divide a $o(xy)$. Esto es también una contradicción. Deducimos que la hipótesis se cumple para $\overline{G}$, como queríamos ver.

Sea $\overline{N} = \mathbf{O}_\pi(\overline{G})$. Como G es contraejemplo minimal, por el párrafo anterior, tenemos que $\overline{x} \in \overline{N}$. Como $\mathbf{O}_\pi(G) = 1$, tenemos que $\mathbf{O}_\pi(N) = 1$. Ahora, usando el Teorema de Schur-Zassenhaus, tenemos que N es el producto semidirecto de un π'-grupo normal R y un π-grupo T que actúa sobre R. Afirmamos que T actúa fielmente sobre R. Observamos que podemos escribir $\mathbf{C}_N(R) = \mathbf{Z}(R) \times X$, para algún π-subgrupo de Hall normal X de N. Como $\mathbf{O}_\pi(N) = 1$, deducimos que $X = 1$ y la acción de T sobre R es fiel. Consideramos $H = \langle x\rangle R$. Como $[x, R] \neq 1$, deducimos del Lema 4.2 que existe un π-elemento en $xR - \{x\}$. Por tanto, existe un elemento no trivial $y \in R$ tal que r no divide a $o(xy)$. Esto contradice nuestra hipótesis, luego $R = 1$.

Paso 3: Afirmamos que $G = \langle x\rangle F$, donde F es el socle de G.

Sabemos que $F = K_1 \times \cdots \times K_t$, donde $\{K_1, \ldots, K_t\}$ son los subgrupos normales minimales de G y K_i es un producto directo de copias de algún grupo simple no abeliano para todo i. Además, por los Pasos 1 y 2, sabemos que $\mathbf{F}(G) = 1$. Por tanto, $\mathbf{C}_G(F) = 1$ y todos los grupos simples que son factores directos de F no son π-grupos (por el Paso 1).

Suponemos que $H = \langle x\rangle F < G$. Observamos que los factores de composición no abelianos de H son factores de composición de G. La hipótesis se conserva para H y deducimos que $x \in \mathbf{O}_\pi(H)$. Como $\mathbf{O}_\pi(H) \cap F \leq \mathbf{O}_\pi(F) = 1$, tenemos que $H = \langle x\rangle \times F$ y x actúa trivialmente sobre F. En este caso,

$x \in \mathbf{C}_G(F) = 1$ y entonces $x = 1$. Esto es una contradicción con el hecho que G es un contraejemplo. Por tanto, $H = G$ y hemos probado este paso.

Paso 4: Afirmamos que F es un subgrupo normal minimal de G.

Suponemos, como en el Paso 3, que $F = K_1 \times \cdots \times K_t$ con $t > 1$. Como $\mathbf{C}_G(F) = 1$, entonces $x \notin \mathbf{C}_G(F)$ y existe algún $i \in \{1, \ldots, t\}$ tal que x no centraliza K_i. La hipótesis se conserva para $\langle x\rangle K_i$ y obtenemos una contradicción como en el Paso 3.

En este punto, tenemos que $G = \langle x\rangle K$, donde K es el único subgrupo normal minimal de G y K es el producto directo de n copias de un grupo simple no abeliano S, para algún entero n.

Paso 5: Afirmamos que $n = 1$.

Suponemos que $K = S_1 \times \cdots \times S_n$ para algún entero $n > 1$, donde $S_i \cong S$ para todo i. Sabemos que $\langle x\rangle$ actúa transitivamente sobre $\{S_1, \ldots, S_n\}$. Como G no es un π-grupo, podemos tomar un primo $q \in \pi'$ divisor de $|S|$ y un q-elemento $y \in S_1$ no trivial. Tenemos que $y^x \in S_j$ para algún $j \neq 1$ es un q-elemento. Por ello, $[y, x] = y^{-1}y^x$ es también un q-elemento y a su vez $[y, x]^{-1} = [x, y]$. Ahora, como $x^y = x[x, y]$ es un π-elemento, deducimos de nuestra hipótesis que $[x, y] = 1$. Por tanto, x centraliza todos los q-elementos de S_1. Similarmente, x centraliza todos los q-elementos de S_j para todo j. Como S_j es simple, S_j está generado por sus q-elementos, así x centraliza S_j para todo j y deducimos que $G = \langle x\rangle \times K$. Esto contradice el Paso 1.

Por tanto, tenemos que $G = \langle x\rangle S$ para algún grupo simple no abeliano S, y recordamos que π es un subconjunto propio no vacío de $\pi(G)$. Finalmente, por la Conjetura 2.11, tenemos que existe un y q-elemento, con $q \in \pi'$ tal que q no divide a $o(xy)$, lo cual contradice la hipótesis, completando la prueba. □

Como consecuencia de este teorema tenemos el Teorema G. En efecto, si los factores de composición no abelianos son esporádicos, alternados o de tipo Lie en característica π', la Conjetura 2.11 se cumple para todos los π-elementos x, por el Teorema 2.12. Por otra parte, observamos que lo que se ha hecho en esta demostración es probar que un contraejemplo minimal a "para todo $q \in \pi'$ y para todo $1 \neq y \in G$ q-elemento, q divide a $o(xy)$ implica que $x \in \mathbf{O}_\pi(G)$" es uno de los grupos almost-simple $\langle x\rangle S$ para los cuales no está demostrada la Conjetura 2.11.

Como consecuencia del teorema anterior, obtenemos el siguiente corolario.

COROLARIO 4.4. *Sean G un grupo y p un primo. Sea $x \in G$ un p-elemento. Suponemos que la Conjetura 2.11 es cierta para todos los p-elementos de todos los grupos cuyo socle es un factor de composición de G. Entonces las siguientes afirmaciones son equivalentes:*

(i) *Para todo $q \neq p$ y todo q-elemento no trivial $y \in G$, se tiene que*
$$\pi(o(x)o(y)) \subseteq \pi(o(xy)).$$

(ii) *Para todo $q \neq p$ y todo q-elemento no trivial $y \in G$, se tiene que*

$$\pi(o(x)o(y)) = \pi(o(xy)).$$

Demostración. Obviamente, (ii) implica (i). Supongamos que es cierto (i), entonces en particular, para todo $q \neq p$ y para todo y q-elemento no trivial de G, se tiene que q divide a $o(xy)$. Aplicando el Teorema 4.3 para $\pi = \{p\}$, se tiene que $x \in \mathbf{O}_p(G)$. Sea $y \in G$ un q-elemento, para algún $q \neq p$ primo. Entonces podemos considerar $H = \mathbf{O}_p(G)\langle y \rangle$. Por tanto, $xy \in H$, luego $\{p, q\} \subseteq \pi(o(xy)) \subseteq \{p, q\}$ y obtenemos (ii). □

4.3. Más resultados

Para acabar este capítulo vamos a ver la prueba original del Teorema 4.3 para grupos p-resolubles.

Teorema 4.5. *Sea G un grupo p-resoluble, con p un primo y sea $x \in G$ un p-elemento. Entonces $x \in \mathbf{O}_p(G)$ si y solo si para todo p'-elemento $y \in G$ de orden potencia de primo, $\pi(o(y)) \subseteq \pi(o(xy))$.*

Demostración. Empezamos suponiendo que $x \in \mathbf{O}_p(G)$. Sea $y \in G$ un q-elemento, para algún primo $q \neq p$. Entonces $xy \in \mathbf{O}_p(G)\langle y \rangle$. Si suponemos que q no divide a $o(xy)$, se tiene que $xy \in \mathbf{O}_p(G)$, por tanto, $y \in \mathbf{O}_p(G)$, lo cual es una contradicción. Se deduce que $\pi(o(y)) \subseteq \pi(o(xy))$, como queríamos demostrar.

Veamos ahora el recíproco. Vamos a trabajar por inducción sobre $|G|$. En primer lugar, observamos que la hipótesis se hereda para subgrupos que contienen a x. Además, si x cumple que $\pi(o(y)) \subseteq \pi(o(xy))$ para todo y q-elemento, para todo primo $q \neq p$, entonces x^g también lo cumple para todo $g \in G$. En efecto, se tiene que $o(x^g y) = o(xy^{g^{-1}})$ y, entonces,

$$\pi(o(x^g y) = \pi(o(xy^{g^{-1}})) \supseteq \pi(o(y^{g^{-1}})) = \pi(o(y)).$$

De forma análoga, se puede ver que x^{-1} cumple la hipótesis.

Veamos que puede suponerse que $\mathbf{O}_{p'}(G) \leq \mathbf{Z}(G)$. Suponemos que $G = \mathbf{O}_{p'}(G)\langle x \rangle$. Sea q un primo distinto de p. Como $\langle x \rangle$ actúa coprimamente sobre $\mathbf{O}_{p'}(G)$, existe un subgrupo $\langle x \rangle$-invariante $Q \in \mathrm{Syl}_q(G)$, es decir, que satisface $Q^x = Q$. Sea $y \in Q$. Entonces escribimos $x^y = x[x, y]$ donde notamos que $[x, y] \in Q$. Como x^y es un p-elemento, se tiene que el orden del producto de x y un q-elemento es una potencia de p, esto contradice la hipótesis. Se deduce que $[x, y] = 1$. Por tanto, $x \in \mathbf{C}_G(y)$ para todo $y \in Q$, y por ello, $x \in \mathbf{C}_G(Q)$. Como esto se verifica para todo primo $q \neq p$, obtenemos que $G = \mathbf{O}_{p'}(G) \times \langle x \rangle$, entonces $x \in \mathbf{O}_p(G)$ y concluimos la prueba. Por tanto, podemos suponer que $\mathbf{O}_{p'}(G)\langle x \rangle < G$ y entonces, por inducción, $x \in \mathbf{O}_p(\mathbf{O}_{p'}(G)\langle x \rangle)$. Esto implica que $x \in \mathbf{C}_G(\mathbf{O}_{p'}(G))$. Ahora bien, si $\mathbf{C}_G(\mathbf{O}_{p'}(G)) < G$, entonces aplicando de nuevo inducción, obtenemos que $x \in \mathbf{O}_p(\mathbf{C}_G(\mathbf{O}_{p'}(G)))$, luego $x \in \mathbf{O}_p(G)$ y obtendríamos el resultado. Entonces $\mathbf{C}_G(\mathbf{O}_{p'}(G)) = G$, es decir, $\mathbf{O}_{p'}(G) \leq \mathbf{Z}(G)$.

Denotamos $N = \mathbf{O}_{p'p}(G)$ y $K = \mathbf{O}_{p'pp'}(G)$. Como $\mathbf{O}_{p'}(G) \leq \mathbf{Z}(G)$, sabemos que $N = \mathbf{O}_p(G) \times \mathbf{O}_{p'}(G)$, con $\mathbf{O}_p(G) > 1$. Además, podemos considerar que $N < G$, si no ya tendríamos el resultado, y por tanto, $K/N = \mathbf{O}_{p'}(G/N) > 1$. En particular, $x \notin K$ (en caso contrario, $x \in N$ y se tendría el resultado). Entonces, fijado un primo $q \neq p$, como $\langle x \rangle$ actúa coprimamente sobre K/N, existe un q-subgrupo de Sylow QN/N de K/N que es $\langle x \rangle$-invariante, para algún $Q \in \mathrm{Syl}_q(K)$. Esto implica que $Q^x \leq QN$. Sea $y \in Q$. Entonces $(yN)^x = y^x N \in QN/N$ y, en particular, $y^x \in QN$. Por otro lado, $QN = Q\mathbf{O}_p(G)\mathbf{O}_{\{p,q\}'}(G)$, con $\mathbf{O}_{\{p,q\}'}(G) \leq \mathbf{Z}(G)$. Entonces podemos escribir $y^x = y'tz$, para algún $y' \in Q$, $t \in \mathbf{O}_p(G)$, $z \in \mathbf{O}_{\{p,q\}'}(G)$. Como $y^x = y(x^{-1})^y x$, entonces $(y')^{-1}y(x^{-1})^y x = tz$ y por tanto,

$$((y')^{-1}y)(x^{-1})^y = (tx^{-1})z.$$

Observamos que en la igualdad anterior, $(y')^{-1}y$ es un q-elemento, $(x^{-1})^y$ es un p-elemento que cumple la propiedad, (tx^{-1}) es un p-elemento, ya que $t \in \mathbf{O}_p(G)$, y z es un $\{p,q\}'$-elemento. Como z es central, $(tx^{-1})z$ es un q'-elemento. Sabemos, por hipótesis, que q divide a $o(((y')^{-1}y)(x^{-1})^y)$, lo cual nos lleva a una contradicción con lo anterior. Entonces, deducimos que $(y')^{-1}y = 1$, es decir, $y = y'$ y así, $(yN)^x = ytzN = yN$. Por tanto, hemos obtenido que $(yN)^x = yN$ para todo q-elemento $y \in G$, es decir, la acción de $\langle x \rangle$ sobre QN/N es trivial. Como esto es cierto para todo primo $q \neq p$, concluimos que $[xN, K/N] = 1$, es decir, $[xN, \mathbf{O}_{p'}(G/N)] = 1$. Por último, como $\mathbf{O}_p(G/N) = 1$, por Hall-Higman se tiene que $\mathbf{C}_{G/N}(\mathbf{O}_{p'}(G/N)) \leq \mathbf{O}_{p'}(G/N)$. Entonces $xN \in \mathbf{O}_{p'}(G/N)$, lo que implica que $x \in N$ ya que x es un p-elemento. Así, $x \in \mathbf{O}_p(G)$ y se concluye la prueba. $\square$

Capítulo 5

Clases de conjugación y caracteres

5.1. Introducción

A partir del resultado de Baumslag y Wiegold sobre órdenes de elementos, es natural considerar las siguientes versiones de caracteres y clases.

Hipótesis 2. Sea G un grupo tal que $\chi(xy) = \chi(x)\chi(y)$ para todo par de elementos no triviales $x, y \in G$ con $(o(x), o(y)) = 1$ y para todo $\chi \in \mathrm{Irr}(G)$.

Hipótesis 3. Sea G un grupo tal que $(xy)^G = x^G y^G$ para todo $x, y \in G$ con $(o(x), o(y)) = 1$.

La Hipótesis 2 ya ha sido estudiada por Guralnick y A. Moretó en [**16**], donde prueban el siguiente teorema que clasifica los grupos que cumplen la condición de caracteres.

Teorema 5.1 (Guralnick-Moretó). *Sea G un grupo. Entonces la propiedad $\chi(xy) = \chi(x)\chi(y)$ para todo par de elementos no triviales $x, y \in G$ con $(o(x), o(y)) = 1$ y para todo $\chi \in \mathrm{Irr}(G)$ se cumple si y solo si G es un grupo de orden potencia de primo, un grupo abeliano o G tiene la siguiente estructura:*

(i) *$G = AP$ donde $A > 1$ es un p'-grupo cíclico y P es un p-subgrupo de Sylow normal para algún primo p.*
(ii) *Si $C = \mathbf{C}_P(A)$ y $D = [A, P]$, entonces $P = CD$ con C abeliano, $D \lhd G$ y $C \cap D = 1$.*
(iii) *La acción de A sobre D es Frobenius.*

Observamos que la condición sobre caracteres implica la de clases de conjugación. En efecto, sean x, y elementos de G de orden coprimo. Sea $z = x^a y^b \in x^G y^G$ para algún $a, b \in G$, entonces

$$\chi(z) = \chi(x^a y^b) = \chi(x^a)\chi(y^b) = \chi(x)\chi(y) = \chi(xy),$$

donde la segunda igualdad se obtiene por hipótesis. Así, $z \in (xy)^G$, entonces $x^G y^G \subseteq (xy)^G$. Deducimos que $(xy)^G = x^G y^G$. Por tanto, los grupos que cumplen la Hipótesis 2 también cumplen la Hipótesis 3. Luego, gracias al Teorema de Guralnick y Moretó, hemos obtenido familias de grupos que cumplen la hipótesis de clases.

Por otro lado, no es la primera vez que se estudian condiciones similares sobre clases. Anterioremente, E. Dade y M. Yadav [**10**] clasificaron los grupos tales que $(xy)^G = x^G y^G$ para todo $x, y \in G$ con $x^G \neq (y^{-1})^G$.

Teorema 5.2 (Dade-Yadav). *Sea G un grupo. Entonces G satisface que $(xy)^G = x^G y^G$ para todo $x, y \in G$ con $x^G \neq (y^{-1})^G$ si y solo si es isomorfo a uno de los grupos siguientes:*

(i) *Cualquier grupo abeliano.*
(ii) *Un p-grupo de Camina no abeliano, para algún primo p, es decir, un p-grupo con un subgrupo normal propio no trivial N tal que cada coclase no trivial de N está contenida en una clase de conjugación de G.*
(iii) *Los grupos $F^{\times}[F^{+}]$, para algún cuerpo finito F con $|F| > 2$.*
(iv) *El grupo $Q_8[C_3 \times C_3]$.*

Observamos que los grupos que cumplen la Hipótesis de Dade y Yadav también satisfacen la Hipótesis 3 y, por tanto, los grupos obtenidos en el teorema anterior son también ejemplos de grupos que cumplen nuestra hipótesis de clases.

Nos gustaría clasificar los grupos que cumplen la Hipótesis 3 pero solo hemos podido obtener los siguientes resultados.

Teorema I. *Sea G un grupo tal que $(xy)^G = x^G y^G$ para todo elemento $x, y \in G$ con $(o(x), o(y)) = 1$, entonces G es resoluble.*

El siguiente teorema clasifica los grupos que cumplen la condición de clases en el caso que G sea un grupo *no nilpotente minimal por cocientes*, es decir, un grupo no nilpotente tal que G/N es nilpotente para cualquier subgrupo normal no trivial N de G. Denotamos por *qmnn*-grupo a estos grupos no nilpotentes minimales por cocientes.

Teorema J. *Sea G un qmnn-grupo. Entonces las siguientes afirmaciones son equivalentes:*

(i) *G es un grupo de Frobenius con núcleo p-elemental abeliano, para algún primo p que divide al orden de G, y complemento nilpotente.*
(ii) *G cumple que para todos los elementos $x, y \in G$ con $(o(x), o(y)) = 1$,*
$$(xy)^G = x^G y^G.$$

Hemos trabajado con la hipótesis de que G sea un *qmnn*-grupo por el hecho de que dado un grupo no nilpotente G que cumple la Hipótesis 3, entonces existe un subgrupo normal M de G de forma que G/M es un *qmnn*-grupo y por tanto, podemos averiguar la estructura de dicho grupo cociente.

Por otro lado, queremos destacar que la prueba del Teorema I no involucra la Clasificación de los Grupos Simples Finitos. Sin embargo, si exigimos que los elementos tengan orden potencia de primo en la hipótesis, entonces sí es necesario recurrir a la Clasificación para probar ese resultado, el cual podemos encontrarlo en [**16**]. Además, el Teorema 5.1 es también cierto si debilitamos de nuevo la hipótesis a los elementos de orden potencia de primo, como puede verse en el mismo artículo.

Los resultados originales de este capítulo se han obtenido en colaboración con A. Beltrán.

5.2. Clases de conjugación

Empezamos recordando la definición del multiplicador a derecha de Dade y Yadav [**10**]. Sean G un grupo y S un subconjunto de G, se define $M_G(S) = \{g \in G \mid Sg = S\}$. Como se indica en [**10**, p. 32], tenemos el siguiente resultado.

Lema 5.3. *Sean G un grupo y S un subconjunto de G. Entonces $M_G(S)$ es un subgrupo de G y $|M_G(S)|$ divide a $|S|$.*

Ahora, vamos a demostrar el Teorema I, el cual reescribimos a continuación. Este teorema no depende de la Clasificación de los Grupos Simples Finitos, tan solo depende del Teorema A del Capítulo 3.

Teorema 5.4. *Sea G un grupo tal que $(xy)^G = x^G y^G$ para todos los elementos $x, y \in G$ con $(o(x), o(y)) = 1$ entonces G es resoluble.*

Demostración. Sea G un contraejemplo minimal. Como la hipótesis se hereda a grupos cocientes, si N es un normal minimal de G, entonces G/N es resoluble. Deducimos que N es un grupo no resoluble y, por tanto, no nilpotente. Por el Teorema A existen elementos $x, y \in N$ de orden potencia de primo y órdenes coprimos tales que $\pi(o(x)o(y)) \nsubseteq \pi(o(xy))$. Por tanto, al menos una de las siguientes afirmaciones es cierta: $(o(xy), o(x)) = 1$ o $(o(xy), o(y)) = 1$.

Supongamos, sin pérdida de generalidad, que $(o(xy), o(y)) = 1$. Así, podemos aplicar la hipótesis a los elementos xy e y^{-1}. Obtenemos que

$$(xy)^G (y^{-1})^G = (xyy^{-1})^G = x^G.$$

Además, aplicando la hipótesis $(xy)^G = x^G y^G$ en la ecuación anterior, obtenemos que

$$x^G y^G (y^{-1})^G = x^G.$$

Ahora, como $y^G (y^{-1})^G$ es un subconjunto de $M_G(x^G)$, por el Lema 5.3, el subgrupo que genera está contenido en $M_G(x^G)$ y, por tanto, su orden divide a $|x^G|$. Además, $|x^G| < |N|$. Así, tenemos un subgrupo normal en G de orden menor estricto que N con N normal minimal, entonces $\langle y^G (y^{-1})^G \rangle = 1$. Esto implica que $y \in \mathbf{Z}(G)$, pero esto es una contradicción. □

El siguiente objetivo es probar el Teorema J, el cual recordamos a continuación.

Teorema 5.5. *Sea G un qmnn-grupo. Entonces las siguientes afirmaciones son equivalentes:*

(i) *G es un grupo de Frobenius con núcleo p-elemental abeliano, para algún primo p que divide al orden de G, y complemento nilpotente.*

(ii) *G cumple que para todos los elementos $x, y \in G$ con $(o(x), o(y)) = 1$,*
$$(xy)^G = x^G y^G.$$

NOTA 5.6. Observamos que unas leves variaciones de la estructura de los grupos de (i) hace que deje de cumplirse la condición (ii). Por ejemplo, sea
$$G = NH = \langle x, y, \alpha \mid x^7 = y^{13} = 1, x^\alpha = x^2, y^\alpha = y^3, xy = yx \rangle,$$
donde $N \cong C_7 \times C_{13}$ y $H \cong C_3$. Este grupo es un grupo de Frobenius con núcleo abeliano, pero no p-grupo, y no cumple la Hipótesis 3. Veámoslo. Se tiene que $x^G = \{x, x^2, x^4\}$ e $y^G = \{y, y^3, y^9\}$. Como N es abeliano, se tiene que $\mathbf{C}_G(xy) = N$. Entonces
$$|(xy)^G| = |G : \mathbf{C}_G(xy)| = |G : N| = 3$$
y $(xy)^G \subsetneq x^G y^G$, ya que el conjunto $x^G y^G$ tiene 9 elementos.

Además, observamos que el resultado también es falso para grupos quasi-Frobenius con núcleo p-grupo y complemento nilpotente. Recordamos que un grupo *quasi-Frobenius* es aquel que su cociente por el centro es un grupo de Frobenius. Basta pensar en $G = \mathrm{SL}(2, 3)$. Este grupo es tal que $G/\mathbf{Z}(G) \cong \mathsf{A}_4$ es un grupo de Frobenius y no cumple la Hipótesis 3. Sean
$$x = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$
de forma que $o(x) = 3$, $o(y) = 4$. Se tiene que $o(xy) = 3$ pero en $x^G y^G$ hay elementos de orden 6, luego $(xy)^G \neq x^G y^G$.

Antes de comenzar con la prueba, necesitamos algunos lemas que nos serán de utilidad. En primer lugar, recordamos el Teorema 6.34 de [**23**] en el cual se determina cómo son los caracteres de los grupos de Frobenius.

TEOREMA 5.7. *Sea G un grupo de Frobenius con núcleo N. Entonces*

(a) *Para $\varphi \in \mathrm{Irr}(N)$, con $\varphi \neq 1_N$, tenemos que $I_G(\varphi) = N$ y $\varphi^G \in \mathrm{Irr}(G)$.*

(b) *Para $\chi \in \mathrm{Irr}(G)$ con $N \nsubseteq \ker(\chi)$, tenemos que $\chi = \varphi^G$ para algún $\varphi \in \mathrm{Irr}(N)$.*

La utilidad de conocer cómo son los caracteres de un grupo de Frobenius se debe a la siguiente equivalencia entre la condición de clases y una nueva relación de caracteres.

PROPOSICIÓN 5.8. *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

(i) *Para todo par de elementos $x, y \in G$ con $(o(x), o(y)) = 1$ se cumple que $(xy)^G = x^G y^G$.*

(ii) *Para todo par de elementos $x, y \in G$ con $(o(x), o(y)) = 1$ y todo $\chi \in \mathrm{Irr}(G)$, se cumple que $\chi(xy)\chi(1) = \chi(x)\chi(y)$.*

DEMOSTRACIÓN. Ver el Lema 2.3 de [**16**] o el Lema 1 de [**31**]. □

El siguiente resultado es un caso más general de una de las implicaciones del Teorema J.

Lema 5.9. *Si G es un grupo de Frobenius con núcleo p-grupo, para algún primo p que divide al orden de G, y complemento nilpotente, entonces G cumple la Hipótesis 3.*

Demostración. Sea G un grupo de Frobenius, $G = HN$, con el núcleo N p-grupo, para algún primo p que divide al orden de G, y H un complemento nilpotente. Queremos ver que para todo $x, y \in G$ con $(o(x), o(y)) = 1$ y para todo $\chi \in \mathrm{Irr}(G)$, se cumple que $\chi(xy)\chi(1) = \chi(x)\chi(y)$. Podemos suponer que $x, y \neq 1$. Por ser G un grupo de Frobenius, sus elementos están en N o en un conjugado de H, por ello, tenemos únicamente los dos siguientes casos a estudiar.

Caso 1. Tomamos $x \in N$, $y \in H$. (Si y está en algún conjugado H^g distinto de H, simplemente consideramos $G = H^g N$.)

Por definición de G, se tiene que x es un p-elemento y que y es un p'-elemento. Sea $\chi \in \mathrm{Irr}(G)$ tal que $N \leq \ker(\chi)$. Entonces $\overline{\chi} \in \mathrm{Irr}(G/N)$ con $\overline{\chi}(gN) = \chi(g)$ para cualquier $g \in G$. De esta forma, se tiene que

$$\begin{cases} \chi(xy) = \overline{\chi}(xyN) = \overline{\chi}(yN) = \chi(y), \\ \quad \chi(x) = \overline{\chi}(xN) = \overline{\chi}(N) = \chi(1). \end{cases}$$

Por tanto, $\chi(xy)\chi(1) = \chi(y)\chi(x)$.

Ahora, consideramos que $N \not\leq \ker(\chi)$ entonces, por el apartado (b) del Teorema 5.7, tenemos que $\chi = \varphi^G$ con $\varphi \in \mathrm{Irr}(N)$. Como $y \notin N$, entonces $\chi(y) = 0$, por definición del carácter inducido. Por otro lado, $xy \notin N$ luego $\chi(xy) = 0$. En caso contrario, $x^{-1}(xy) = y \in N$, lo cual es una contradicción. Por tanto, $\chi(xy)\chi(1) = 0 = \chi(y)\chi(x)$.

Caso 2. Tomamos $x \in H$, $y \in H^g$, para algún $g \in G$. Podemos suponer que $g \in N$.

En este caso se tiene que x, y son p'-elementos de orden coprimo. Sea $\chi \in \mathrm{Irr}(G)$.

Empezamos suponiendo que $N \leq \ker(\chi)$. Como $y \in H^g$, entonces existe un $y_1 \in H$ tal que $y = y_1^g$ y por definición de carácter, $\chi(y) = \chi(y_1^g) = \chi(y_1)$.

A la vez se tiene que $y = y_1 y_1^{-1} g^{-1} y_1 g = y_1[y_1, g]$, con $[y_1, g] \in N$. Entonces, $xy = xy_1^g = xy_1[y_1, g]$ y por tanto,

$$\chi(xy) = \chi(xy_1[y_1, g]) = \overline{\chi}(xy_1[y_1, g]N) = \overline{\chi}(xy_1N) = \chi(xy_1).$$

Además, como $xy = xy_1[y_1, g]$, se tiene que $xyN = xy_1N$ y se dan las siguientes relaciones.

$$\begin{cases} \overline{\chi}(xy_1N) = \overline{\chi}(xyN) = \chi(xy), \\ \qquad \overline{\chi}(N) = \chi(1), \\ \qquad \overline{\chi}(xN) = \chi(x), \\ \quad \overline{\chi}(y_1N) = \chi(y_1) = \chi(y). \end{cases}$$

Ahora, como G/N es nilpotente, se cumple la condición para $\overline{\chi}$ y entonces $\overline{\chi}(xy_1N)\overline{\chi}(N) = \overline{\chi}(xN)\overline{\chi}(y_1N)$. Por tanto, usando las relaciones anteriores obtenemos que $\chi(xy)\chi(1) = \chi(x)\chi(y)$.

Para concluir, suponemos que $N \nleq \ker(\chi)$, luego $\chi = \varphi^G$ con $\varphi \in \mathrm{Irr}(N)$. Entonces como $x, y \notin N$, se tiene que $\chi(x) = \chi(y) = 0$. Además, $xy \notin N$ (ya que $xy = xy_1[y_1, g]$ con $x, y_1 \in H$ de órdenes coprimos no triviales y $[y_1, g] \in N$) y, por tanto, $\chi(xy) = 0$. □

Vamos a ver también el siguiente lema, el cual es cierto también para grupos p-resolubles.

Lema 5.10. *Sea G un grupo resoluble con $\mathbf{O}_{p'}(G) = 1$. Entonces todo p'-elemento g no trivial se puede descomponer como el producto de un p'-elemento no trivial y un p-elemento no trivial, de la siguiente forma: $g = g^{x^{-1}}[g, x]^{x^{-1}}$.*

Demostración. Sea g un p'-elemento no trivial. Por Hall-Higman, como $\mathbf{O}_{p'}(G) = 1$, se tiene que $\mathbf{C}_G(\mathbf{O}_p(G)) \leq \mathbf{O}_p(G)$. Por tanto, $\langle g \rangle$ actúa fielmente sobre $\mathbf{O}_p(G)$. Sea $x \in \mathbf{O}_p(G)$ tal que $gx \neq xg$. Tenemos que $g^x = g[g, x]$ y $[g, x] \in \mathbf{O}_p(G) - \{1\}$. Por tanto, $g = g^{x^{-1}}[g, x]^{x^{-1}}$, donde $1 \neq g^{x^{-1}}$ es un p'-elemento y $1 \neq [g, x]^{x^{-1}}$ es un p-elemento. □

Por último, usaremos el siguiente lema.

Lema 5.11. *Sea $G = HN$ con $N \trianglelefteq G$ y $H \cap N = 1$. Sea $x \in H$. Entonces*

$$\mathbf{C}_G(x) = \mathbf{C}_N(x)\mathbf{C}_H(x).$$

Demostración. Ver Lema 1 de [9]. □

Por el Lema 5.9, tenemos probado que (i) implica (ii) en el Teorema J, por tanto, solo falta ver el siguiente resultado.

Teorema 5.12. *Sea G un qmnn-grupo tal que para todo par de elementos $x, y \in G$ de órdenes coprimos se tiene que $x^G y^G = (xy)^G$. Entonces G es un grupo de Frobenius con núcleo p-elemental abeliano, para algún primo p que divide al orden de G, y complemento nilpotente.*

Demostración. Vamos a fragmentar la prueba en 3 pasos.

Paso 1. El residual nilpotente K de G es el único normal minimal de G.

Por hipótesis, para todo subgrupo normal no trivial N de G, se tiene que G/N es nilpotente. Como por definición K es el menor subgrupo normal para el que sucede eso, $K \leq N$. Por tanto, K es un normal minimal que está contenido en cualquier subgrupo normal no trivial. Por tanto, K es el único normal minimal de G.

Paso 2. $G = KD$ con K p-elemental abeliano y D un p'-subgrupo nilpotente.

Por el paso anterior y por ser G resoluble, K es un p-subgrupo abeliano elemental de G, para algún primo p. Además como $\overline{G} = G/K$ es nilpotente, se tiene que $\overline{G} = \overline{G_p} \times \overline{G_{p'}}$, con $\overline{G_p}$ el único p-subgrupo de Sylow de $\overline{G}$ y $\overline{G_{p'}}$ su único p'-subgrupo de Hall. Se sigue que la imagen inversa de $\overline{G_p}$ es un p-subgrupo de Sylow normal P de G que contiene a K. Ahora, por el Teorema de Schur-Zassenhaus existe un subgrupo D de G que es un complemento para P en G, es decir, $G = PD$. Entonces $\overline{G_{p'}} = DK/K \cong D$. Así, como $G/K = P/K \times DK/K$, se tiene que D es un p'-subgrupo de G nilpotente que normaliza a P y que centraliza a $P/K = \overline{G_p}$. Esto implica que $[P, D] \leq K$. Además, por ser P normal, $[\mathbf{N}_P(D), D] \leq P$ y también $[\mathbf{N}_P(D), D] \leq D$, entonces $[\mathbf{N}_P(D), D] \leq P \cap D = 1$. Se concluye que $\mathbf{N}_P(D)$ centraliza a D y que $\mathbf{N}_P(D) = \mathbf{C}_P(D)$. Por otra parte, por acción coprima, sabemos que $P = \mathbf{C}_P(D)[P, D]$, y como $[P, D] \leq K$, se tiene que $P = \mathbf{C}_P(D)K = \mathbf{N}_P(D)K$. Por tanto,

$$G = PD = K(\mathbf{N}_P(D) \times D).$$

Veamos que $\mathbf{C}_K(D) = 1$. Por ser $1 \neq \mathbf{Z}(P) \trianglelefteq G$ y por la minimalidad de K, se tiene que $K \leq \mathbf{Z}(P)$. Por un lado tenemos que $K = [K, D] \times \mathbf{C}_K(D)$, ya que K es abeliano y D actúa sobre K de forma coprima. Por otro lado, se tiene que $K = [K, G] = [K, PD] = [K, D]$. Entonces $\mathbf{C}_K(D) = 1 = \mathbf{N}_K(D)$.

Veamos finalmente que $K = P$ y por tanto, $G = KD$. Como $K \leq \mathbf{Z}(P)$ y $P = K\mathbf{C}_P(D)$, se tiene que $\mathbf{C}_P(D) \trianglelefteq P$. Además, D normaliza $\mathbf{C}_P(D)$. Entonces $\mathbf{C}_P(D) \trianglelefteq G$. Si $\mathbf{C}_P(D) \neq 1$, por la minimalidad de K deducimos que $K \leq \mathbf{C}_P(D)$. Entonces $P = \mathbf{C}_P(D)$ pero entonces $G = P \times D$ y G sería nilpotente, contradicción. Se concluye que $\mathbf{C}_P(D) = 1$ y por tanto, $P = K$.

Paso 3. La acción de D sobre K es de Frobenius.

Tenemos que $K = \mathbf{O}_p(G)$ y $\mathbf{O}_{p'}(G) = 1$. Por el Lema 5.10 tenemos que para todo p'-elemento g de G no trivial, $g = g^{x^{-1}}[g, x]^{x^{-1}}$, con g p'-elemento e $y = [g, x] \in \mathbf{O}_p(G)$. Por tanto, aplicando la hipótesis, $g^G = g^G y^G$. Como y^G es un subconjunto de $M_G(x^G)$, por el Lema 5.3, tenemos que $|\langle y^G \rangle|$ divide a $|g^G|$. Pero $\langle y^G \rangle \leq K$ es un subgrupo normal de G, entonces por la minimalidad de K, $\langle y^G \rangle = K$. Por tanto, $|K|$ divide a $|g^G| = |G : \mathbf{C}_G(g)|$.

Por ser g un p'-elemento, g está en un conjugado de D. Podemos suponer que $g \in D$. Entonces tenemos que $g \in D$ con $G = KD$, $K \trianglelefteq G$ y $K \cap D = 1$. Por el Lema 5.11 se deduce que $\mathbf{C}_G(g) = \mathbf{C}_K(g)\mathbf{C}_D(g)$. Entonces $|K|$ divide a $|G : \mathbf{C}_G(g)|$ y

$$|G : \mathbf{C}_G(g)| = |KD : \mathbf{C}_K(g)\mathbf{C}_D(g)| = |K : \mathbf{C}_K(g)||D : \mathbf{C}_D(g)|.$$

Como $|D : \mathbf{C}_D(g)|$ es coprimo con $|K|$, se tiene que $|K|$ divide a $|K : \mathbf{C}_K(g)|$, lo que implica que $\mathbf{C}_K(g) = 1$.

Por tanto, hemos visto que para todo p'-elemento g de G no trivial, $\mathbf{C}_K(g) = 1$. Por tanto, la acción de D sobre K es de Frobenius. □

Corolario 5.13. *Sea G un grupo no nilpotente que satisface la Hipótesis 3. Entonces existe un subgrupo normal M de G tal que $\overline{G} = G/M$ es* *un grupo de Frobenius con núcleo p-grupo abeliano, para algún primo p que divide al orden de $\overline{G}$, y complemento nilpotente.*

Demostración. Podemos tomar M normal en G y maximal respecto a la condición de que $\overline{G}$ no es nilpotente, así $\overline{G}$ es un *qmnn*-grupo y aplicamos el Teorema J. □

5.3. Más resultados

En esta sección, vamos a presentar algunos resultados y cuestiones relacionados con la Hipótesis 3.

Al igual que hemos hecho en capítulos anteriores, tiene sentido preguntarse qué sucede si debilitamos la condición de clases a los elementos de orden potencia de primo. Los siguientes resultados podemos encontrarlos en [**1**] y [**16**] y ambos dependen de la Clasificación de los Grupos Simples Finitos. El primero de ellos da una condición suficiente para que un grupo sea p-resoluble. El segundo, obtiene como conclusión que G tenga factores de composición de orden divisible por dos primos. Este resultado está relacionado con el Teorema 2.8.

Teorema 5.14 (Guralnick-Moretó). *Sea G un grupo y sea p un primo. Si $(xy)^G = x^G y^G$ para todo p-elemento $x \in G$ y para todo p'-elemento $y \in G$ de orden potencia de primo. Entonces G es p-resoluble.*

Teorema 5.15 (Guralnick-Moretó-N. Ahanjideh). *Sean $p \neq q$ dos primos y sea G un grupo. Suponemos que $(xy)^G = x^G y^G$ para todo $x \in G$ p-elemento e $y \in G$ q-elemento. Entonces G no tiene factores de composición de orden divisible por pq.*

A diferencia de lo que ocurre en el Teorema 5.1, todos los grupos nilpotentes cumplen la hipótesis sobre clases (Hipótesis 3) y, por ello, no podemos obtener información adicional sobre el subgrupo de Fitting de los grupos que cumplen dicha hipótesis. Quizás en el caso de que G no sea nilpotente y no tenga productos directos sí podamos encontrar un resultado que nos aporte información sobre el subgrupo de Fitting $\mathbf{F}(G)$ o los cocientes por el Fitting. De hecho, nos parece que la respuesta a la siguiente cuestión puede ser cierta, a partir de la observación de los grupos que cumplen la Hipótesis 3 obtenidos con la librería *SmallGroups* en GAP [**12**].

Cuestión 6. ¿Es cierto que si G no es un producto directo y cumple que $(xy)^G = x^G y^G$ para todo $x, y \in G$ con $(o(x), o(y)) = 1$, entonces $G/\mathbf{F}(G)$ es metacíclico y que hay como mucho dos primos en $|G/\mathbf{F}(G)|$? En general, ¿es cierto que $G/\mathbf{F}(G)$ es metabeliano?

En el Apéndice B mostramos algunos ejemplos que hemos seleccionado de entre los grupos que cumplen la Hipótesis 3.

A partir de ahora, vamos a trabajar con longitudes de clases de conjugación. El Teorema 2.2 de [**16**] prueba que (i) es equivalente a (ii) en el siguiente resultado, el cual es una nueva caracterización de los grupos nilpotentes.

TEOREMA 5.16. *Sea G un grupo entonces las siguientes afirmaciones son equivalentes:*

(i) *G es nilpotente,*
(ii) *$|x^G||y^G| = |(xy)^G|$ para todo par de elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$,*
(iii) *$|x^G||y^G|$ divide a $|(xy)^G|$ para todo par de elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$,*
(iv) *$|x^G||y^G| \leq |(xy)^G|$ para todo par de elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$,*

Necesitaremos el siguiente lema para probar el teorema anterior.

LEMA 5.17. *Sean p un primo y G un grupo. Un p-subgrupo de Sylow de G es un factor directo de G si y solo si para todo p-elemento x y para todo p'-elemento y de orden potencia de primo, x e y conmutan, En particular, G es nilpotente si y solo si para todos los elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$, se tiene que x e y conmutan.*

DEMOSTRACIÓN. Ver Lema 2.1 de [**16**]. □

DEMOSTRACIÓN DEL TEOREMA 5.16. Si G es nilpotente entonces todo par de elementos de orden coprimo conmutan. Sea $x \in G$ un p-elemento y sea y un q-elemento, para ciertos primos $p \neq q$ de $\pi(G)$. Como todos los subgrupos de Sylow de G son normales, por hipótesis, entonces todo r-elemento está contenido en el r-subgrupo de Sylow, para cada r de $\pi(G)$. Por tanto, $R \leq \mathbf{C}_G(x)$, para todo r-subgrupo de Sylow R con $r \neq p$. Por otro lado, $P \leq \mathbf{C}_G(y)$ con $P \in \mathrm{Syl}_p(G)$. Por tanto, $\mathbf{C}_G(x)\mathbf{C}_G(y)$ contiene todos los subgrupos de Sylow de G pero G es el producto directo de estos. Concluimos que $G = \mathbf{C}_G(x)\mathbf{C}_G(y)$. De esta forma,

$$|G : \mathbf{C}_G(x) \cap \mathbf{C}_G(y)| = |G : \mathbf{C}_G(x)||G : \mathbf{C}_G(y)|.$$

Además, por hipótesis,

$$|G : \mathbf{C}_G(x) \cap \mathbf{C}_G(y)| = |G : \mathbf{C}_G(xy)|,$$

se deduce que $|x^G||y^G| = |(xy)^G|$.

Ahora, como (ii) implica (iii) y (iii) implica (iv), vamos a ver que (iv) implica (i). Suponemos que $|x^G||y^G| \leq |(xy)^G|$ para todo par de elementos $x, y \in G$ de orden potencia de primo con $(o(x), o(y)) = 1$. Tomamos $x, y \in G$ de esta forma. Por el Lema 5.17, basta ver que x e y conmmutan. Tenemos que

$$|x^G||y^G| = |G : \mathbf{C}_G(x)||G : \mathbf{C}_G(y)| \leq |G : \mathbf{C}_G(xy)| = |(xy)^G|.$$

Por tanto,

$$|G : \mathbf{C}_G(x) \cap \mathbf{C}_G(y)| \leq |G : \mathbf{C}_G(x)||G : \mathbf{C}_G(y)| \leq |G : \mathbf{C}_G(xy)|.$$

Así tenemos que $|\mathbf{C}_G(xy)| \leq |\mathbf{C}_G(x) \cap \mathbf{C}_G(y)|$. Como es cierto siempre que $\mathbf{C}_G(x) \cap \mathbf{C}_G(y) \leq \mathbf{C}_G(xy)$, se obtiene que $\mathbf{C}_G(x) \cap \mathbf{C}_G(y) = \mathbf{C}_G(xy)$. Se sigue que $xy \in \mathbf{C}_G(xy) \leq \mathbf{C}_G(y)$ y entonces xy conmuta con y. Deducimos que x e y conmutan. $\square$

A continuación, vemos dos contraejemplos que muestran que no es posible obtener las versiones análogas de los Teoremas C y E del Capítulo 3 para longitudes de clases de conjugación. Sin embargo, podría ser que otras versiones de estos resultados sí puedan ser ciertas.

Ejemplo 5.18. Sean $\pi = \{2, 3\}$ y $G = D_{120}$, el grupo diédrico de orden 120. Este grupo es tal que para todos los 2-elementos x y para todos los 3-elementos y se cumple que $\pi(|x^G||y^G|) \subseteq \pi(|(xy)^G|)$, pero los π-subgrupos de Hall de G son isomorfos a D_{24}, por lo tanto, no son nilpotentes. Así, hemos visto que el Teorema C es falso para longitudes de clases de conjugación.

Ejemplo 5.19. Sean $G = D_{24}$ y $\pi = \{2\}$. Se cumple que las clases de cualquier 3-elemento (es decir, $2'$-elemento) tienen longitud 2. Por tanto, se verifica que $\{2\} = \pi(|y^G|) \subseteq \pi(|(xy)^G|) = \{2, 3\}$, para todo 2-elemento x. Sin embargo, G no tiene un 2-subgrupo de Sylow normal.

Para concluir con este capítulo, vamos a ver el siguiente resultado relacionado con los primos que dividen la longitud de una clase de conjugación. Este teorema nos sirvió de inspiración para obtener el Teorema 3.23. El resultado que vamos a probar es la versión π del Teorema 5 de [**29**]. Este teorema afirma que dado un grupo G y un primo p divisor del orden de G, se tiene que p no divide a $|x^G|$ para todo p'-elemento x de orden potencia de primo si y solo si $G = \mathbf{O}_p(G) \times \mathbf{O}_{p'}(G)$. Este resultado necesita el Teorema 1 de [**11**] que afirma que dado un grupo G que actúa transitivamente sobre un conjunto Ω con $|\Omega| > 1$, entonces existen un primo r y un r-elemento $g \in G$ tales que g actúa libre de puntos fijos sobre Ω, el cual depende de la Clasificación de los Grupos Simples Finitos.

Vamos a ver una reproducción de la prueba ya existente del Teorema 5 de [**29**] pero para un conjunto de primos π y únicamente para los grupos π-separables, ya que en ese caso podemos garantizar las propiedades necesarias sobre los π-subgrupos de Hall. Debido a que la hipótesis no se hereda a subgrupos, vemos complicado utilizar otro razonamiento sin usar el Teorema 1 de [**11**] y tampoco vemos cómo quitar la condición de π-separabilidad.

Teorema 5.20. *Sea G un grupo π-separable, con π un conjunto de primos que dividen el orden de G. Entonces para todo $p \in \pi$, se tiene que $p \nmid |x^G|$ para todo π'-elemento x de G de orden potencia de primo si y solo si $G = H \times K$, donde H es un π-subgrupo de Hall de G y K es un π'-subgrupo de Hall de G.*

Demostración. Es suficiente probar la implicación "solo si", ya que la otra implicación es trivial. En efecto, basta observar que para todo $x \in K$, se tiene que $H \leq \mathbf{C}_G(x)$.

En primer lugar, vamos a ver que G tiene un π-subgrupo de Hall normal. Para ello, suponemos que $|\mathrm{Hall}_\pi(G)| > 1$. Consideramos la acción de G sobre Ω. Sabemos que G actúa transitivamente sobre Ω. Por el Teorema 1 de [**11**], existen un primo r y un r-elemento $g \in G$ tales que g actúa libre de puntos fijos sobre Ω, es decir, para todo $H \in \mathrm{Hall}_\pi(G)$, tenemos que $H^g \neq H$. Ahora, si $r \notin \pi$, para todo $p \in \pi$ se tiene que $p \nmid |g^G|$, por hipótesis. Entonces $|G|_p = |\mathbf{C}_G(g)|_p$ para todo $p \in \pi$ y por tanto, existe un elemento $z \in G$ tal que $H^z \leq \mathbf{C}_G(g)$. Esto implica que $(H^z)^g = H^z$, lo cual es una contradicción. Por tanto, $r \in \pi$, es decir, g es un π-elemento. Entonces existe $x \in G$ tal que $g \in H^x$, lo que implica que $(H^x)^g = H^x$ y llegamos de nuevo a una contradicción que viene de suponer $|\mathrm{Hall}_\pi(G)| > 1$. Por tanto, $H \in \mathrm{Hall}_\pi(G)$ es normal en G.

Ahora, por el Teorema de Schur-Zassenhaus, existe un π'-subgrupo de Hall K de G tal que $G = HK$. Sea $x \in K$ de orden potencia de primo. Entonces $p \nmid |x^G|$ por hipótesis, para todo $p \in \pi$. Por tanto, $H \leq \mathbf{C}_G(x)$. Deducimos que $H \leq \mathbf{C}_G(K)$ y entonces $G = H \times K$. $\square$

Apéndice A

Demostraciones de la Sección 2.3

En primer lugar, vamos a ver la reducción a grupos quasisimples del Teorema 2.8, el cual reescribimos a continuación.

TEOREMA A.1. *Sea G un grupo y sean p y q primos diferentes. Las siguientes afirmaciones son equivalentes:*

(i) *G contiene un factor de composición cuyo orden es divisible por pq.*
(ii) *Existen elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un r-elemento para algún primo $r \neq p, q$ y $xyz = 1$. Además, si p y q son impares, podemos tomar $r = 2$.*

La demostración (ii) implica (i) se puede ver de forma análoga a lo hecho en el Corolario 2.9. Por tanto, vamos a ver cómo es un contraejemplo minimal a la implicación contraria.

TEOREMA A.2. *Sean $p \neq q$ primos. Un contraejemplo minimal a (i) implica (ii) en el Teorema A.1 es un grupo quasisimple con socle un simple minimal de orden divisible por pq.*

Para poder probar este resultado, necesitamos un par de lemas. El primer lema es la Proposición 2.1. de [**18**].

LEMA A.3. *Sean G un grupo y N un p-subgrupo normal no abeliano de G para un primo $p > 2$. Suponemos que N es minimal entre todos los subgrupos normales de G no centrales. Entonces $N/\mathbf{Z}(N)$ tiene un complemento en $G/\mathbf{Z}(N)$. En particular, N no está contenido en $\Phi(G)$.*

El siguiente lema es el Lema 2.2 de [**18**].

LEMA A.4. *Sea p un primo y sea G un grupo generado por los elementos $g_1, \ldots, g_r$. Suponemos que o bien $G = \mathbf{O}^p(G)$ o todos los g_i son p'-elementos. Sea N un p-subgrupo abeliano de G que es un subgrupo normal minimal no central de G. Sea $C_i := [g_i, N]$. Entonces*

$$(g_1C_1)(g_2C_2)\cdots(g_rC_r) = (g_1 \cdots g_r)N. \tag{A.1}$$

Además, todo elemento de g_iC_i es N-conjugado a g_i y está contenido en la coclase g_iN.

DEMOSTRACIÓN TEOREMA A.2. Sea G un contraejemplo minimal. Entonces, G contiene un factor de composición de orden divisible por pq pero no contiene elementos no triviales x, y, z tales que $xyz = 1$, x es un p-elemento, y un q-elemento y z un elemento de orden potencia de un primo r distinto de p, q y si p y q son impares, $r = 2$. Por tanto, cualquier subgrupo propio tampoco contiene esos elementos, ya que sino los contendría G, lo cual sería una contradicción. Además, por ser G minimal, deducimos que todo subgrupo propio no tiene un factor de composición de orden divisible por pq. Veamos que G es quasisimple. Como G/G' es abeliano, entonces no puede contener factores de composición de orden divisible por pq. Por tanto, G' debe tener un factor de composición de orden divisible por pq, ya que G lo tiene. Sin embargo, hemos dicho que todo subgrupo propio de G no contiene uno, por tanto, $G = G'$, es decir, G es perfecto.

Ahora, vamos a ver por reducción al absurdo que $\Phi(G)$ es el mayor subgrupo normal propio de G. Suponemos que existe un subgrupo normal propio N de G tal que $N \nleq \Phi(G)$. Entonces $G = MN$ para M un subgrupo maximal $M < G$. En efecto, como $\Phi(G)$ es la intersección de todos los subgrupos maximales de G y N no está contenido en $\Phi(G)$, sabemos que existe un subgrupo maximal M tal que $N \nleq M$. Entonces $M \lneq NM \leq G$. Como M es maximal, deducimos que $G = MN$. Entonces obtenemos que $M/(M \cap N) \cong MN/N = G/N$. Además, N no contiene elementos no triviales x, y, z tales que x es un p-elemento, y un q-elemento y z un r-elemento con $r \neq p, q$ y si p y q son impares, $r = 2$ y $xyz = 1$. Por la minimalidad de G, N no tiene factores de composición de orden divisible por pq. Por tanto, G/N tiene un factor de composición de orden divisible por pq. Se sigue que M tiene un factor de composición de orden divisible por pq, lo cual es de nuevo una contradicción. Por tanto, $\Phi(G)$ es el mayor subgrupo normal propio de G y $G/\Phi(G)$ es simple.

Por último, veamos que $\Phi(G)$ es central. Suponemos que no lo es. Entonces existe un subgrupo normal propio N en G que no es central. Sea $N \leq \Phi(G)$ un tal subgrupo de orden lo menor posible. Como $N \leq \Phi(G)$ y $\Phi(G)$ es nilpotente, deducimos que N es nilpotente. Por tanto, la minimalidad de N implica que N es un s-grupo para algún primo s. Vamos a ver que $\mathbf{O}_p(G) = \mathbf{O}_q(G) = \mathbf{O}_2(G) = 1$. Suponemos que $\mathbf{O}_p(G) \neq 1$, entonces $\overline{G} = G/\mathbf{O}_p(G)$ tiene un factor de composición de orden divisible por pq ya que $\mathbf{O}_p(G)$ no lo tiene. Por la minimalidad de G, se tiene $\overline{G}$ cumple la tesis. Así, existen elementos no triviales $\overline{x}, \overline{y}, \overline{z} \in \overline{G}$ tales que $\overline{xyz} = \overline{1}$, $\overline{x}$ es un p-elemento, $\overline{y}$ un q-elemento y $\overline{z}$ un elemento de orden potencia de un primo r distinto de p, q y si p y q son impares, $r = 2$. Se puede suponer que x es p-elemento, y es q-elemento y z es r-elemento. Por tanto, $xyz = n \in \mathbf{O}_p(G)$. Entonces $(n^{-1}x)yz = 1$, donde $n^{-1}x$ es un p-elemento, y un q-elemento y z un r-elemento, para algún primo $r \neq p, q$ y si p y q son impares, $r = 2$; lo que nos lleva de nuevo a una contradicción. Deducimos que $\mathbf{O}_p(G) = 1$. Análogamente, observamos que $\mathbf{O}_q(G) = 1$. Ahora, si $p = 2$ o $q = 2$, ya tenemos que $\mathbf{O}_2(G) = 1$. Por tanto, podemos suponer que p y q son primos impares y $r = 2$. Suponemos que $\mathbf{O}_2(G) \neq 1$, entonces $\overline{G} = G/\mathbf{O}_2(G)$ tiene un factor de composición de orden divisible por pq ya que $\mathbf{O}_2(G)$ no lo tiene. Por la minimalidad de G, tenemos que $\overline{G}$ cumple la tesis. Esto implica que existen elementos no triviales $\overline{x}, \overline{y}, \overline{z} \in \overline{G}$ tales que $\overline{x}$ es un p-elemento, $\overline{y}$ un q-elemento y $\overline{z}$ un 2-elemento y $\overline{xyz} = \overline{1}$. Se puede suponer que x es p-elemento, y es q-elemento y z es 2-elemento. Por tanto, $xyz = n \in \mathbf{O}_2(G)$. Entonces $xy(zn^{-1}) = 1$, donde zn^{-1} es un 2-elemento, x un p-elemento e y un q-elemento; lo que nos lleva de nuevo a una contradicción. Por tanto, $\mathbf{O}_2(G) = 1$. Esto implica que $s \neq p, q, 2$. También, por el Lema A.3, tenemos que N es abeliano. Por ello, G/N tiene un factor de composición de orden divisible por pq, lo que implica que G/N cumple el teorema. Por tanto, existen elementos no triviales $x, y, z \in G$ tales que x es un p-elemento, y es un q-elemento, z es un elemento de orden potencia de un primo $r \neq p, q$ y si p y q son impares, $r = 2$ y $xyz = n$ para algún $n \in N$. Sea $L/N = \langle xN, yN, zN \rangle$ para algún subgrupo L de G. Entonces como L/N contiene tales elementos, por la implicación contraria, L/N contiene un factor de composición de orden divisible por pq. En particular, por ser N abeliano, L contiene un factor de composición de orden divisible por pq. Por la minimalidad de G, deducimos que $L = G$. Ahora consideramos $G = \langle x, y, z \rangle N$, y así $G = \langle x, y, z \rangle$ ya que $N \leq \Phi(G)$. Por último, por el Lema A.4, existen elementos conjugados x_1, y_1, z_1 en N de x, y, z, respectivamente, tales que $x_1 y_1 z_1 = 1$. Esto contradice el hecho que G es contraejemplo, por lo que obtenemos que $\Phi(G)$ es central. Concluimos que $G/\mathbf{Z}(G)$ es simple y como G es perfecto, tenemos que G es quasisimple. $\square$

De forma análoga a la reducción anterior, se comprueba que un contraejemplo minimal al hecho que "si un grupo G no es resoluble entonces para algunos $q \neq s$ primos impares, G contiene elementos no triviales x, y, z tales que x es un 2-elemento, $o(y) = p$, $o(z) = s$ y $xyz = 1$" es un grupo quasisimple con socle un simple minimal de orden divisible por $2p$. Como todos los grupos simples son pares, estamos diciendo que un contraejemplo minimal es un grupo quasisimple con socle un simple minimal de orden divisible por p. Por tanto, en este caso, gracias a la clasificación de los grupos simples minimales de Thompson (Teorema 1.3), podemos probar el siguiente teorema (Teorema 2.5) en su totalidad.

Teorema A.5. *Un grupo es resoluble si y solo si no contiene elementos x, y, z no triviales tales que $xyz = 1$ donde x es un 2-elemento y los elementos y, z tienen orden primo impar distinto.*

En primer lugar, vamos a ver la implicación "solo si". De hecho, vamos a ver la siguiente versión más fuerte.

Teorema A.6. *Si G es un grupo resoluble entonces no contiene elementos x, y, z no triviales tales que $xyz = 1$, con x p-elemento, y q-elemento y z r-elemento, para p, q, r primos distintos dividiendo el orden de G.*

Demostración. Sea G un contraejemplo minimal. Así G es resoluble y contiene elementos x, y, z no triviales tales que $xyz = 1$, con x p-elemento, y q-elemento y z r-elemento, para p, q, r primos distintos dividiendo el orden de G. Como G es resoluble y es divisible por al menos 3 primos, entonces G no es simple. Sea N un subgrupo normal no trivial propio de G.

Sea $x \in N$. Siguiendo los pasos de la demostración del Corolario 2.9 llegamos a que $x, y, z \in N$ lo que contradice la minimalidad de G. Análogamente, deducimos que $x, y, z \notin N$. En este caso $xN \in G/N$ es un p-elemento no trivial, $yN \in G/N$ es un q-elemento no trivial y zN es un r-elemento no trivial. De nuevo, tenemos una contradicción con la minimalidad de G. $\square$

Para ver la implicación que nos falta del Teorema A.5, es decir, para probar el teorema en el caso que G sea quasisimple, la clave es el siguiente resultado sobre caracteres.

Como hemos comentado, el libro de Isaacs [**23**] es una excelente introducción a la Teoría de Caracteres. Allí encontraremos la información necesaria para entender la prueba del siguiente lema que aparece como Problema 3.9 de [**23**]. Ahora, para ayudar a la lectura de estas líneas, vamos a recordar cómo es la función ω asociada a un carácter.

Sean G un grupo y $\chi \in \mathrm{Irr}(G)$. Sean $g \in G$ y $K = g^G$ una clase de conjugación. Denotamos por $\mathbf{Z}(\mathbb{C}[G])$ el centro del álgebra de grupo $\mathbb{C}[G]$. Los elementos de $\mathbf{Z}(\mathbb{C}[G])$ son sumas de los elementos de una clase de conjugación de G, es decir, un elemento $\widehat{K} \in \mathbf{Z}(\mathbb{C}[G])$ asociado a K viene dado por $\widehat{K} = \sum_{g \in K} g$. La función ω_χ es un homomorfismo de álgebras que depende de χ y está definida de $\mathbf{Z}(\mathbb{C}[G])$ en $\mathbb{C}$, de forma que $\mathfrak{X}(z) = \omega_\chi(z)\mathbf{I}$, para todo $z \in \mathbf{Z}(\mathbb{C}[G])$, donde $\mathbf{I}$ es la matriz identidad de $\mathrm{GL}(n, \mathbb{C})$. Se puede ver que ω_χ es un homomorfismo y que es lineal en $\mathbb{C}$. Entonces, calculando trazas en la ecuación $\mathfrak{X}(K) = \omega_\chi(K)\mathbf{I}$ obtenemos que

$$\omega_\chi(\widehat{K}) = \frac{\chi(g)|K|}{\chi(1)}.$$

Lema A.7. *Sean $K_i = g_i^G, \ldots, K_t = g_t^G$ las clases de conjugación de G con $g_i \in G$ los representantes. Sean $\widehat{K_i}$ las sumas formales asociadas a cada K_i. Sean $a_{ij\nu}$ enteros definidos por*

$$\widehat{K_i}\widehat{K_i} = \sum_\nu a_{ij\nu}\widehat{K_\nu}.$$

Entonces

$$a_{ij\nu} = \frac{|K_i||K_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_\nu)}}{\chi(1)}$$

Demostración. Sea $\chi \in \mathrm{Irr}(G)$. Sabemos que los $\widehat{K_r}$ forman una base de $\mathbf{Z}(\mathbb{C}[G])$ para $r = 1, \ldots, t$ y, por ello, tenemos que $\widehat{K_i}\widehat{K_j} = \sum_\nu a_{ij\nu}\widehat{K_\nu}$. Ahora, aplicamos el homomorfismo ω_χ a la igualdad anterior y obtenemos que

$$\frac{|K_i||K_j|\chi(g_i)\chi(g_j)}{\chi(1)^2} = \sum_{\nu=1}^{t} a_{ij\nu}\frac{|K_\nu|\chi(g_\nu)}{\chi(1)}.$$

Multiplicamos a ambos lados de la igualdad por $\overline{\chi(g_r)}$ para algún $g_r \in K_r$ con $r \in \{1,\dots,t\}$ y realizamos la suma para cada $\chi \in \mathrm{Irr}(G)$. Así tenemos la siguiente expresión:

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{|K_i||K_j|\chi(g_i)\chi(g_j)\overline{\chi(g_r)}}{\chi(1)} = \sum_{\chi\in\mathrm{Irr}(G)}\sum_{\nu=1}^{t} a_{ij\nu}|K_\nu|\chi(g_\nu)\overline{\chi(g_r)}.$$

Reescribimos el lado derecho de la igualdad intercambiando los sumatorios, $\sum_{\nu=1}^{t} a_{ij\nu}|K_\nu| \sum_{\chi\in\mathrm{Irr}(G)} \chi(g_\nu)\overline{\chi(g_r)}$. Ahora, aplicando la segunda relación de ortogonalidad, la segunda suma es 0 salvo cuando $\nu = r$, en tal caso suma $|\mathbf{C}_G(g_\nu)|$. Por tanto, la expresión anterior queda de esta forma $a_{ij\nu}|K_\nu||\mathbf{C}_G(g_\nu)| = a_{ij\nu}|G|$. Concluimos que

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{|K_i||K_j|\chi(g_i)\chi(g_j)\overline{\chi(g_r)}}{\chi(1)} = a_{ij\nu}|G|.$$

Deducimos así el resultado. □

Escribimos $\chi(K_i) = \chi(g)$ para $g \in K_i$. A partir del lema anterior, deducimos que si

$$\Sigma(x,y,z) := \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(K_i)\chi(K_j)\chi(K_\nu)}{\chi(1)} \neq 0, \tag{A.2}$$

entonces existen elementos $x \in K_i$, $y \in K_j$ tales que $xy \in K_\nu$.

Recordamos que estamos viendo que si G es un grupo quasisimple con socle uno de los grupos de la lista de Thompson (Teorema 1.3) $\mathrm{PSL}(2,q)$, $\mathrm{Sz}(q)$ o $\mathrm{PSL}(3,3)$ entonces existen elementos no triviales $y, z \in G$ tales que $o(y) = p$, $o(z) = s$ para algunos primos $p, s \neq 2$ tales que $yz = x$ es un 2-elemento. Para ello, usando el lema anterior, queremos encontrar en la tabla de caracteres dos columnas correspondientes a las clases de conjugación que denotaremos K_p y K_s de elementos de orden primo impar p y s, respectivamente, y una columna de 2-elementos correspondiente con la clase K_2, tales que

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(K_p)\chi(K_s)\chi(K_2)}{\chi(1)} \neq 0.$$

A continuación, vamos a ver las tablas de caracteres de los siguientes grupos quasisimples. En cuanto a la presentación del interior de las tablas de caracteres, queremos recalcar que la cantidad de caracteres irreducibles de cada fila coincide con el número de clases de conjugación que hay en la columna correspondiente.

Las Tablas 1 y 2 están extraídas de [35] y representan las tablas de caracteres de los grupos $\mathrm{SL}(2,q)$ para q par e impar, respectivamente. En ambas tablas, denotamos por ρ y σ las raíces primitivas de la unidad de grado $q-1$ y $q+1$, respectivamente.

Tabla de caracteres de $\mathrm{PSL}(2,q)$, con q par				
Número	1	1	$\frac{1}{2}(q-2)$	$\frac{1}{2}q$
$\mathrm{Irr}(G) \setminus x^G$	I	U	A_i	S_j
1_G	1	1	1	1
St_G	q	0	1	-1
χ_α	$q+1$	1	$\rho^{\alpha i}+\rho^{-\alpha i}$	0
η_β	$q-1$	-1	0	$-(\sigma^{\beta j}+\sigma^{-\beta j})$

TABLA 1

En particular, sabemos que los grupos simples $\mathrm{PSL}(2,q)=\mathrm{SL}(2,q)$ con q par, tienen una clase de orden 2, la hemos denotado por U. El orden de los elementos de las clases A_i, S_j divide a $q-1$, $q+1$, respectivamente. Como hemos comentado anteriormente, por la estructura de la tabla, se tiene que los paramétros $i,\alpha \in \left\{1,\dots,\frac{q-2}{2}\right\}$ y $j,\beta \in \left\{1,\dots,\frac{q}{2}\right\}$.

Tabla de caracteres de $\mathrm{SL}(2,q)$, con q impar						
Número	1	1	2	2	$\frac{1}{2}(q-3)$	$\frac{1}{2}(q-1)$
$\mathrm{Irr}(G) \setminus x^G$	I	-I	U,U'	$-U,-U'$	A_k	S_l
1_G	1	1	1	1	1	1
St_G	q	q	0	0	1	-1
ρ_i	$\frac{1}{2}(q+1)$	$\frac{1}{2}(q+1)e$	z_i	z_ie	$(-1)^i$	0
π_j	$\frac{1}{2}(q-1)$	$\frac{-1}{2}(q-1)e$	z_j	z_je	0	$-(-1)^j$
χ_α	$q+1$	$(-1)^\alpha(q+1)$	1	e_α	$\rho^{\alpha k}+\rho^{-\alpha k}$	0
η_β	$q-1$	$(-1)^\beta(q-1)$	-1	$-e_\beta$	0	$-(\sigma^{\beta l}+\sigma^{-\beta l})$

TABLA 2

En la Tabla 2, se tiene que $z_i = \frac{1}{2}(1 \pm \sqrt{eq})$, donde $e=+1$, si $q \equiv 1 \pmod 4$ y $e=-1$, si $q \equiv -1 \pmod 4$. Análogamente, $z_j = \frac{1}{2}(-1 \mp \sqrt{eq})$. Los valores $e_\alpha, e_\beta \in \{\pm 1\}$ y dependen del carácter en el que se evalúe. Si $q=r^f$, los elementos de U y U' tienen orden r, y los de $-U$ y $-U'$ orden $2r$. Luego, por la estructura de la tabla, se tiene que $i,j \in \{1,2\}$. El orden de los elementos de las clases A_k, S_l divide a $q-1$, $q+1$, respectivamente. De nuevo, como el número de caracteres de grado $q+1$ y $q-1$ coincide con el número de clases A_k y S_l, respectivamente, se tiene que $k,\alpha \in \left\{1,\dots,\frac{q-3}{2}\right\}$ y $l,\beta \in \left\{1,\dots,\frac{q-1}{2}\right\}$.

Tabla de caracteres de Sz(q), con $q=2^{2m+1}$						
Número	1	1	2	$\frac{1}{2}(q-2)$	$\frac{1}{4}(q+r)$	$\frac{1}{4}(q-r)$
Irr(G) $\setminus x^G$	1	σ	ρ,ρ^{-1}	τ_0	τ_1	τ_2
χ_1	1	1	1	1	1	1
χ_2	q^2	0	0	1	-1	-1
χ_{3l}	$\frac{r}{2}(q-1)$	-$\frac{r}{2}$	$\pm\frac{r}{2}\sqrt{-1}$	0	1	-1
χ_{4i}	q^2+1	1	1	$\xi_0^i(\pi_0)$	0	0
χ_{5j}	$(q-r+1)(q-1)$	r-1	-1	0	-$\xi_1^j(\pi_0)$	0
χ_{6k}	$(q-r+1)(q-1)$	-r-1	-1	0	0	-$\xi_2^k(\pi_0)$

Tabla 3

La Tabla 3 está extraída de [39], donde r es tal que $2q=r^2$. Los elementos de la clase σ tienen orden 2. Sabemos que los grupos $Sz(q)$ tienen 2 clases de elementos de orden 4, son ρ y ρ^{-1}. También sabemos que tiene subgrupos cíclicos de orden $q-1, q+r+1$ y $q-r+1$ que originan las clases τ_0, τ_1 y τ_2, respectivamente. Los valores $\xi_u^v(\pi_0)$ son elementos del cuerpo $\mathbb{Q}(w_u)$, donde w_u son n-raíces primitivas de la unidad, con $n=q-1, p+r+1$ y $q-r+1$, respectivamente, en función de $u=0,1,2$. Los parámetros de la Tabla 3 toman los valores $l=1,2$, $i\in\left\{1,\dots,\frac{q-2}{2}\right\}$, $j\in\left\{1,\dots,\frac{q+r}{4}\right\}$ y $k\in\left\{1,\dots,\frac{q-r}{4}\right\}$.

Tabla de caracteres de PSL$(3,3)$								
Número	1	1	1	4	1	1	2	1
Irr(G) $\setminus x^G$	1A	3A	3B	13A$_i$	2A	6A	8A$_j$	4A
χ_1	1	1	1	1	1	1	1	1
χ_2	12	3	0	-1	4	1	0	0
χ_3	13	4	1	0	-3	0	-1	1
χ_{4i}	16	-2	1	z_i	0	0	0	0
χ_5	26	-1	-1	0	2	-1	0	2
χ_{6j}	26	-1	-1	0	-2	1	$\pm2\sqrt{-1}$	0
χ_7	27	0	0	1	3	0	-1	-1
χ_8	39	3	0	0	-1	-1	1	-1

Tabla 4

Por último, tenemos la tabla de PSL$(3,3)$ que la podemos encontrar en [6]. Aquí, hemos denotado por z_i a un elemento del cuerpo $\mathbb{Q}(w)$ con w una raíz 13-ésima de la unidad, que varía en función de $i\in\{1,\dots,4\}$. Por la estructura de la tabla, $j\in\{1,2\}$.

Una vez hemos visto las tablas de caracteres de los grupos quasisimples con socle un grupo simple minimal, podemos concluir con la prueba del

Teorema A.5. Para ello, vamos a ver el siguiente lema, que es similar al Lema 3.3 de [18].

LEMA A.8. (i) *Sea* $G = \mathrm{SL}(2,q)$ *con* $q \geq 4$*, respectivamente* $G = \mathrm{Sz}(q)$ *con* $q \geq 8$*. Entonces existen elementos no triviales* x, y, z *tales que* $xyz = 1$*,* x *es un* 2*-elemento,* $o(y) = p$*,* $o(z) = s$ *para primos impares* p, s *distintos.*

(ii) *Sea* G *un grupo quasisimple con todos los subgrupos propios resolubles. Entonces existen elementos no triviales* x, y, z *tales que* $xyz = 1$*,* x *es un* 2*-elemento,* $o(y) = p$*,* $o(z) = s$ *para primos impares* p, s *distintos.*

DEMOSTRACIÓN. Se pretende encontrar x, y, z tales que $xyz = 1$, x es un 2-elemento, $o(y) = p$, $o(z) = s$ para primos impares p, s distintos. Para ello, usaremos el Lema A.7 y, por tanto, nuestro propósito será encontrar los adecuados x, y, z tales que $\Sigma(x, y, z) \neq 0$ (Ecuación A.2).

Empezamos viendo el apartado (i). Sea $G = \mathrm{Sz}(q)$ con $q \geq 8$ y $r^2 = 2q$. Entonces podemos tomar x de orden 2, y de orden primo p impar con p dividiendo a $q + r + 1$ o $q - r - 1$, es decir, y perteneciendo a las clases τ_1 o τ_2, respectivamente, y z en la clase τ_0 de orden primo impar s tal que $s|q-1$.

Ahora, si tomamos $G = \mathrm{SL}(2,q) = \mathrm{PSL}(2,q)$, en el caso de q par, basta tomar x de orden 2 con $x \in U$, $y \in A_1$ con $o(y) = p$ y $p|(q-1)$ y $z \in S_1$ de orden primo impar s, coprimo con p, tal que $s|q+1$.

Si $G = \mathrm{SL}(2,q)$, $q = r^f$ y r es un primo impar, entonces debemos considerar dos casos. Si $4|q-1$, entonces podemos tomar x de orden 4 en la clase A_1, $y \in S_1$ de forma que $o(y) = p$, con $p|\frac{q+1}{2}$ y z en U o U' donde $o(z) = r$. Si $4|q+1$, entonces elegimos x en la clase S_1 de orden 4, y en A_1 de forma que $o(y) = p$, con $p|\frac{q-1}{2}$ y z en U o U' donde $o(z) = r$.

Observando las tablas para cualquiera de los casos anteriores, obtenemos que el único sumando de la suma de la ecuación del Lema A.7 que no se anula es el correspondiente al carácter trivial del grupo. El resto de sumandos se anulan ya que todos los caracteres no triviales se anulan en alguna de las clases mencionadas. Por tanto, queda:

$$\Sigma(x, y, z) = \frac{1 \cdot 1 \cdot 1}{1_G(1)} \neq 0.$$

Veamos ahora el apartado (ii). Es suficiente probar el resultado para G, el recubrimiento de Schur de $G/\mathbf{Z}(G)$. Por tanto, por el Teorema 1.3, podemos suponer que G es uno de los siguientes grupos: $\mathrm{SL}(2,q)$, $\mathrm{PSL}(3,3)$, $\mathrm{Sz}(q)$, o $2^2 \cdot \mathrm{Sz}(8)$. Si $G = \mathrm{SL}(2,q)$ o $\mathrm{Sz}(q)$, entonces por el apartado (i) ya lo tenemos. Para $G = \mathrm{PSL}(3,3)$, podemos elegir un elemento x de orden 2, y de orden 3 (de la clase 3B) y z de orden 13. Observando la tabla podemos comprobar de nuevo que la suma $\Sigma(x, y, z)$ es no nula gracias al carácter trivial. Para concluir, consideramos $G = 2^2 \cdot \mathrm{Sz}(8)$. En este caso, podemos encontrar su tabla de caracteres en [**6**], y se puede ver que es suficiente tomar x un 2-elemento no central, y un elemento de orden 7 y z un elemento de orden 13. Nuevamente, el único sumando que se mantiene no nulo en $\Sigma(x, y, z)$ es el correspondiente al carácter trivial. □

La demostración dada en esta sección tiene el fin de ilustrar algunas de las ideas que han sido usadas para probar el Teorema 2.12 en el caso que el socle sea un grupo simple de tipo Lie (en la característica adecuada). A continuación, probamos el Teorema 2.12 en los casos restantes, es decir, cuando S es un grupo alternado o un grupo espóradico.

Comenzamos probando el teorema en el caso que el socle sea un grupo esporádico. Para ello hemos creado el siguiente programa en GAP [**12**], basado en el Lema A.7. Inicialmente, creamos la función *ppart* de un número.

```
ppart:=function(n,p)
 local a;
 a:=1;
 while IsInt(n/p) do
   n:=n/p;a:=a*p;
 od;
 return a;
end;
```

Ahora, procedemos con la explicación del uso del programa creado para probar la Conjetura 2.3 de [**3**]. Esta conjetura es equivalente a la Conjetura 2.11.

Conjetura (Conjetura 2.3 de [**3**]). Sea G un grupo almost-simple con socle simple no abeliano S, y sea p un primo divisor de $|G|$. Suponemos que $G = \langle x \rangle S$, donde x es un p'-elemento no trivial. Entonces existe un p-elemento no trivial $y \in G$ tal que p no divide a $o(xy)$.

Primero, ponemos en la lista llamada “simples” los nombres de los grupos esporádicos y los grupos almost-simple cuyo socle sea un grupo esporádico, usando para ello el comando:

```
AllCharacterTableNames();
```

Segundo, creamos dos listas: *cp* que contiene los órdenes de los representantes de clases que tienen orden una potencia del primo p (el p-elemento “y” en la conjetura anterior) y *cpp* que contiene aquellos cuyos órdenes no son divisibles por p (el p'-elemento “x” en la conjetura anterior).

En los bucles, construimos una lista llamada “lista” que contiene los órdenes de los elementos xy (usamos el Lema A.7 para ello).

Por último, pedimos al programa que muestre los casos donde todo elemento en “lista” sea divisible por p, ya que en ese caso no se cumpliría la conjetura.

```
for G in simples do
 t:=CharacterTable(G);
 ir:=Irr(t);
 ocr:=OrdersClassRepresentatives(t);
 pd:=PrimeDivisors(Size(t));

 for p in pd do
  cp:=[];
  for i in [1..Length(ocr)] do
    if ppart(ocr[i],p)=ocr[i] and ocr[i]<>1 then
        Add(cp,i);
    fi;
  od;
  cpp:=[];
  for j in [1..Length(ocr)] do
    if Gcd(ocr[j],p)=1 and ocr[j]<>1 then
        Add(cpp,j);
    fi;
  od;

  for x in cpp do
    lista:=[];
    for y in cp do
      for i in [1..Length(ocr)] do
        k:=0;
        for j in [1..Length(ir)] do
           k:=k + (ir[j][x]*ir[j][y]*ir[j][i])/ir[j][1];
        od;

        if k<>0 then
           Add(lista, ocr[i]);
        fi;
      od;
    od;

    lista:=Set(lista);
    l:=0;
    for m in lista do
       if Gcd(m,p)=p then
           l:=l+1;
       fi;
    od;
       if l=Length(lista) then
           Display([G, p, ocr[x], x]);
       fi;
```

```
  od;
 od;
od;
```

Ahora, vamos a ver que el Teorema 2.12 es cierto cuando G tiene por socle un grupo alternado. Como la prueba es por inducción, usamos el programa anterior para comprobar el teorema en el caso que S sea un grupo alternado de grado entre 5 y 9.

TEOREMA A.9. *La Conjetura 2.11 es cierta si $S = \mathsf{A}_n$ para algún $n \geq 5$.*

Antes de probar el teorema anterior, vamos a enunciar un par de lemas que usaremos. Sea $\sigma \in \mathsf{S}_n$. Denotamos por m_σ al número de puntos que no son fijados por σ y por n_σ al número de ciclos en su descomposición como el producto de ciclos disjuntos de longitud mayor que 1.

LEMA A.10 (Lema 2 de [20]). *Sea $\sigma \in \mathsf{S}_n$ y sea*

$$(a_1 \dots a_{m_1})(a_{m_1+1} \dots a_{m_2}) \cdots (a_{m_{n_\sigma-1}} \dots a_{m_\sigma})$$

la descomposición de σ como el producto de ciclos disjuntos de longitud mayor que 1. Entonces σ puede expresarse como el siguiente producto de dos ciclos de longitud m_σ y n_σ:

$$\sigma = (a_1 a_2 \dots a_{m_\sigma})(a_{m_{n_\sigma-1}+1} \dots a_{m_2+1} a_{m_1+1} a_1).$$

Por tanto, $m_\sigma + n_\sigma$ es un número par si y solo si $\sigma \in \mathsf{A}_n$ y es impar si $\sigma \in \mathsf{S}_n - \mathsf{A}_n$.

LEMA A.11 (Teorema 7 de [20]). *Sea $\sigma \in \mathsf{S}_n$ y sean $l_1, l_2 \in \mathbb{N}$, $n \geq l_1 \geq l_2 \geq 2$. Entonces $\sigma = C_1 C_2$, donde C_1 y C_2 son ciclos en S_n de longitudes l_1, l_2, respectivamente, si y solo si se da una de las siguientes opciones:*

(i) *$n_\sigma = 2$ y l_1, l_2 son las longitudes de los ciclos en la descomposición de σ como producto de ciclos disjuntos y $l_1 + l_2 = m_\sigma$,*
(ii) *$l_1 + l_2 = m_\sigma + n_\sigma + 2s$ para algún $s \in \mathbb{N} \cup \{0\}$ y $l_1 - l_2 \leq m_\sigma - n_\sigma$.*

LEMA A.12 (Corolario 3.1 de [7]). *Para $n \neq 5$, toda permutación impar de S_n puede expresarse como un producto de un l-ciclo y un $(l+1)$-ciclo si y solo si*

$$\left[\frac{3n}{4}\right] \leq l \leq n-1, \quad n \equiv 1 \ \textit{or} \ 2 \pmod 4,$$
$$\left[\frac{3n}{4}\right] - 1 \leq l \leq n-1, \quad n \equiv 0 \ \textit{or} \ 3 \pmod 4.$$

LEMA A.13 (Proposición 4 de [22]). *En el grupo simétrico S_n, toda permutación par es el producto de dos ciclos de longitud n.*

DEMOSTRACIÓN DEL TEOREMA A.9. Sea $G = \langle x \rangle S$ un grupo almost-simple con socle S, donde $x \in G$ no trivial. Sea $p \in \pi(G) - \pi(o(x))$. Nuestro objetivo es encontrar un p-elemento no trivial $y \in \mathsf{A}_n \leq G$ tal que xy es un

p'-elemento. Procedemos por inducción sobre $n \geq 5$. Como hemos comentado anteriormente, el teorema ha sido comprobado para $5 \leq n \leq 9$. Por tanto, por inducción, $n \geq 10$, $\mathsf{A}_n \leq G \leq \mathsf{S}_n$, $p \leq n$.

Para cualquier $\omega \in \mathsf{S}_n$, sea $m_\omega := |\{1 \leq i \leq n \mid \omega(i) \neq i\}|$ el número de puntos que mueve ω y sea n_ω el número de ciclos no triviales en la descomposición de ω como el producto de ciclos disjuntos. Observamos que $m_\omega \geq 2n_\omega$, ya que ω tiene n_ω ciclos disjuntos de longitud al menos dos. Por el Lema A.10, se tiene que $\omega \in \mathsf{A}_n$ si y solo si $2 \mid (m_\omega - n_\omega)$. Además, dados dos enteros $l_1, l_2 \geq 2$, por el Lema A.11, tenemos que ω puede escribirse como el producto uv donde $u \in \mathsf{S}_n$ es un l_1-ciclo y $v \in \mathsf{S}_n$ un l_2-ciclo si y solo si al menos una de las siguientes afirmaciones se da:

(a) $n_\omega = 2$ y ω es un producto disjunto de un l_1-ciclo y un l_2-ciclo;
(b) $l_1 + l_2 = m_\omega + n_\omega + 2s$ para algún $s \in \mathbb{Z}_{\geq 0}$ y $|l_1 - l_2| \leq m_\omega - n_\omega$.

En primer lugar, consideramos que $p = n$. Si x es una permutación impar, entonces por el Lema A.12, tenemos que $x = zy^{-1}$, donde y es un n-ciclo y z es un $(n-1)$-ciclo. Deducimos que $xy = z$ es un p'-elemento. Suponemos que $x \in \mathsf{A}_n$. Como $2|(m_x - n_x)$ y $m_x \geq 2n_x$, tenemos que $2 \leq m_x - n_x$. Por tanto, aplicando (b) para $l_1 = n-2$ y $l_2 = n$, tenemos que $x = zy^{-1}$, donde $y \in \mathsf{A}_n$ es un n-ciclo y z es un $(n-2)$-ciclo. Obtenemos que $xy = z$ es un p'-elemento.

De ahora en adelante, podemos suponer que $p \leq n - 1$. Aplicando la hipótesis de inducción a $n - 1$, tenemos probado el teorema en el caso de que x tenga un punto fijo, es decir, $m_x = n - 1$. Así pues podemos suponer que $m_x = n$.

Consideramos el caso que $n_x = 1$, es decir, x está formado por un único ciclo no trivial. Además, como $m_x = n$, deducimos que x es un n-ciclo. Por el Lema A.13, todo elemento de A_n es un producto de dos n-ciclos. Por tanto, para $p > 2$, podemos encontrar un p-ciclo $y \in \mathsf{A}_n$ tal que $y = x^{-1}z$ para algún n-ciclo z, de forma que $xy = z$ es un p'-elemento, ya que z es un n-ciclo y $p \leq n-1$. Ahora si $p = 2$, podemos encontrar un $1 \neq y \in \mathsf{A}_n$, un conjugado $(12)(34)$, tal que $y = x^{-1}z$ para algún n-ciclo z. Por tanto, $xy = z$ es un $2'$-elemento.

A continuación, consideramos el caso $n_x \geq 2$ y $p \leq n/2$. Entonces, como $m_x = n$, podemos escribir el p'-elemento $x = \alpha\beta$ como un producto disjunto de (necesariamente) p'-elementos $1 \neq \alpha \in \mathsf{S}_k$ y $1 \neq \beta \in \mathsf{S}_{n-k}$, y observamos que $n > k \geq n/2 \geq \max\{p, 5\}$, ya que $n \geq 10$. Si $p > 2$, entonces por la hipótesis de inducción aplicada al elemento $\alpha \in \mathsf{S}_k$, existe un p-elemento $1 \neq y \in \mathsf{A}_k$ tal que αy es un p'-elemento, por lo que $xy = (\alpha y)\beta$ es un p'-elemento en G. Si $p = 2$, entonces el $2'$-elemento α está contenido en A_k. Aplicando la hipótesis de inducción a $\alpha \in \mathsf{A}_k$, podemos encontrar un 2-elemento $y \in \mathsf{A}_k$ tal que αy es un $2'$-elemento, de donde $xy = (\alpha y)\beta$ es un $2'$-elemento en G.

Ahora podemos suponer que $p < n = m_x < 2p$; en particular, $p \geq 7$ ya que $n \geq 10$. En este caso, $n_x \leq m_x/2 < p$ y $p < m_x + n_x \leq 3m_x/2 < 3p$.

Suponemos primero que $m_x+n_x \neq 2p$. Entonces por (b), podemos encontrar un p-ciclo $y \in \mathsf{A}_n$ y un (m_x+n_x-p)-ciclo z tal que $x = zy^{-1}$, de forma que se obtiene que $xy = z$ es un p'-elemento. Finalmente, suponemos que $m_x+n_x = 2p$. En este caso, de nuevo por (b), podemos encontrar un p-ciclo $y \in \mathsf{A}_n$ y un $(p+2)$-ciclo z tal que $x = zy^{-1}$, completando la prueba. $\square$

Nota A.14. En este teorema basta encontrar un p-elemento y de forma que xy es un p'-elemento, para x p'-elemento, mientras que para probar la Conjetura 2.10 el elemento xy debería ser coprimo con p y con q, ya que en la hipótesis y es ahora un q-elemento y x un p-elemento. Por ello, en algún momento de la prueba, deberíamos obtener también que q divide a $p-2$, lo cual no es cierto para cualesquiera p y q primos. Por ello, esta prueba no es trivialmente adaptable a la Conjetura 2.10.

Apéndice B

Ejemplos

En primer lugar, mostramos algunos grupos resolubles obtenidos en GAP [**12**] que son los grupos de menor orden que no cumplen que para todo $x, y \in G$ tales que $(o(x), o(y)) = 1$, $\pi(o(xy)) \subseteq \pi(o(x)o(y))$. Es decir, los grupos que no cumplen la Hipótesis 1 de la Sección 3.5 tales que todos sus subgrupos propios, cocientes y subcocientes sí la cumplen. Mostramos los grupos de la lista *SmallGroups(n,p)* hasta orden 2000 que nos ofrece el programa, indicando al principio la n y la p, donde n es el orden del grupo y p la posición en la lista de grupos de ese orden. (Recordamos que cualquier grupo no resoluble, tampoco cumple la condición.)

```
150 5 -> ((C5 x C5) : C3) : C2
168 43 -> ((C2 x C2 x C2) : C7) : C3
294 7 -> ((C7 x C7) : C3) : C2
726 5 -> ((C11 x C11) : C3) : C2
750 6 -> (((C5 x C5) : C5) : C3) : C2
810 101 -> ((C3 x C3 x C3 x C3) : C5) : C2
1014 7 -> ((C13 x C13) : C3) : C2
1176 214 -> ((C7 x C7) : Q8) : C3
1210 7 -> ((C11 x C11) : C5) : C2
1500 123 -> ((C5 x ((C5 x C5) : C2)) : C2) : C3
1734 5 -> ((C17 x C17) : C3) : C2
```

En segundo lugar, mostramos algunos grupos que cumplen que para todo elemento $x, y \in G$ con $(o(x), o(y)) = 1$, $(xy)^G = x^G y^G$. Es decir, mostramos algunos de los grupos que cumplen la Hipótesis 3 del Capítulo 5. Aquí tan solo incluimos una pequeña selección que ejemplifica la diversidad de grupos que se obtienen y, por tanto, la dificultad de clasificarlos. Los primeros cuatro ejemplos cumplen también la Hipótesis 2, es decir, son grupos con la estructura del Teorema 5.1. De entre los ejemplos también se encuentran algunos de los grupos del Teorema de Dade y Yadav (Teorema 5.2). Hay otros ejemplos que son productos directos de los grupos anteriores. El resto de los ejemplos no son de ninguno de los tipos mencionados. Al igual que antes, son grupos obtenidos de la lista *SmallGroups(n,p)* que nos ofrece el programa de GAP [**12**], indicando al principio la n y la p y a continuación la estructura del grupo.

```
6 1 -> S3
10 1 -> D10
12 3 -> A4
14 1 -> D14
36 10 -> S3 x S3
60 8 -> S3 x D10
72 41 -> (C3 x C3) : Q8
72 44 -> A4 x S3
84 8 -> S3 x D14
100 13 -> D10 x D10
108 40 -> (C3 x ((C3 x C3) : C2)) : C2
144 120 -> ((C3 x C3) : C4) : C4
200 42 -> ((C5 x C5) : C4) : C2
200 44 -> (C5 x C5) : Q8
300 23 -> ((C5 x C5) : C3) : C4
784 162 -> (C7 x C7) : Q16
1200 962 -> S3 x ((C5 x C5) : Q8)
```

Apéndice C

Bases de Sylow

En este apéndice vamos a estudiar la Cuestión 4, la cual pregunta cuáles son los grupos que satisfacen la propiedad de que todo subgrupo de Sylow es S-semipermutable. Recordamos que un subgrupo H de G es S-semipermutable si conmuta con todos los subgrupos de Sylow de orden coprimo con H. Llamamos *conjunto de representantes de Sylow*, a cualquier conjunto formado por un p-subgrupo de Sylow, para cada primo p que divide a $|G|$. Recordamos que una *base de Sylow* es un conjunto de representantes de Sylow con la propiedad de que conmutan dos a dos. Por tanto, la cuestión anterior es equivalente a preguntarnos cuáles son los grupos que satisfacen la propiedad de que todo conjunto de representantes de Sylow es base de Sylow. Se tiene que un grupo G es resoluble si y solo si contiene una base de Sylow [**24**, p. 90], por tanto, estos grupos son resolubles.

Nuestro objetivo es probar la siguiente condición suficiente para que un grupo G cumpla que todo conjunto de representantes de Sylow es base de Sylow en términos de los números de Sylow.

Teorema C.1. *Sea G un grupo tal que sus números de Sylow son coprimos dos a dos. Entonces G cumple que todo conjunto de subgrupos de Sylow, uno para cada primo divisor del orden del grupo, es una base de Sylow.*

Veamos que el recíproco es falso.

Ejemplo C.2. Sea $G = H \times K$, donde $H \cong D_{14}$ y K es el producto semidirecto de C_3 actuando sobre C_7. Este grupo cumple que todo conjunto de subgrupos de Sylow, uno para cada primo divisor del orden del grupo, es una base de Sylow pero tiene $1, 7, 7$ como números de Sylow.

En primer lugar, observamos que los grupos que cumplen la hipótesis del Teorema C.1 son resolubles.

Lema C.3. *Sea G un grupo tal que sus números de Sylow son coprimos dos a dos. Entones G es resoluble.*

Antes de probar el lema anterior, vamos a definir el grafo de Sylow $\Gamma_S(G)$ de un grupo G. Los vértices de $\Gamma_S(G)$ son los divisores primos de cualquier número de Sylow de G y dos vértices p y q están conectados por un eje si pq divide a algún número de Sylow. El conjunto de números de Sylow, $ns(G)$, está compuesto por los números de Sylow distintos de 1 y tiene cardinal menor o igual que $\pi(G)$. Este grafo fue estudiado por Zhang en [**45**]. En el mismo artículo (Teorema 3) prueba que si el grafo de Sylow de un grupo es disconexo, entonces el grupo no es simple. Nótese que en [**15**] se considera una definición diferente del grafo de Sylow.

Nota C.4. Existen numerosos artículos en los que trabajan con este grafo pero tomando como vértices los divisores primos de los grados de caracteres del grupo o los divisores primos de las longitudes de las clases de conjugación. Se puede ver (en [**28**]) que estos grafos tienen acotado el número de componentes conexas, lo cual no ocurre en el caso del grafo de Sylow. En efecto, siempre se puede crear un grupo de forma que los números de Sylow sean todos los primos que dividen al orden del grupo y entonces, en este caso, habrá tantas componentes conexas como primos en $\pi(G)$.

El siguiente lema, bien conocido, nos proporciona información sobre los números de Sylow de los subgrupos normales y los grupos cocientes de un grupo finito.

Lema C.5. *Sean G un grupo y N un subgrupo normal de G. Sea p un primo. Entonces*

(i) $\nu_p(N)$ *divide a* $\nu_p(G)$.
(ii) $\nu_p(G/N)$ *divide a* $\nu_p(G)$.

Demostración. Sea $P \in \mathrm{Syl}_p(G)$ y sea $PN/N \in \mathrm{Syl}_p(G/N)$. Entonces

$$\begin{aligned}\nu_p(G/N) &= |G/N : \mathbf{N}_{G/N}(PN/N)| = \\ &= |G/N : \mathbf{N}_G(P)N/N| = \\ &= |G : \mathbf{N}_G(P)|/|\mathbf{N}_G(P)N : \mathbf{N}_G(P)| = \\ &= |G : \mathbf{N}_G(P)|/|N : \mathbf{N}_N(P)| = \\ &= \nu_p(G)/|N : \mathbf{N}_N(P)|\end{aligned}$$

Se deduce de forma inmediata que $\nu_p(G/N)$ divide a $\nu_p(G)$. Para ver (i), basta observar que $\mathbf{N}_N(P) = \mathbf{N}_G(P) \cap N$ y que $\nu_p(N) = |N : \mathbf{N}_N(P \cap N)|$ divide a $|N : \mathbf{N}_N(P)|$ ya que $\mathbf{N}_N(P)$ es subgrupo de $\mathbf{N}_N(P \cap N)$. □

Demostración del Lema C.3. Sea G contraejemplo minimal. Queremos ver, en primer lugar, que G no es simple. Si suponemos que hay al menos 2 números de Sylow distintos de 1, entonces el grafo de Sylow asociado a G es disconexo. Ahora, por el Teorema 3 de [**45**] deducimos que G no es simple. Luego, podemos suponer que hay un único número de Sylow distinto de 1. Entonces G tiene como mucho un primo p para el que sus p-subgrupos de Sylow no son normales, para algún primo $p \in \pi(G)$. Por tanto, G es resoluble. Así, hemos probado que G no es simple. Sea N un subgrupo normal minimal de G. Por el lema anterior, sabemos que los números de Sylow de N y de G/N son también coprimos dos a dos. Si N no es resoluble, llegamos a una contradicción con la minimalidad de G. Por tanto, N es abeliano. Como G no es resoluble, entonces G/N no es resoluble y llegamos de nuevo a contradicción con la minimalidad de G. □

Sabemos que dos bases de Sylow cualesquiera de un grupo resoluble son conjugadas, véase, por ejemplo, el Teorema 9.3.2. de [**36**]. Dado π un conjunto de primos tal que $\pi \subseteq \pi(G)$, definimos π-*base de Sylow* como un conjunto de subgrupos de Sylow, uno para cada primo de π, con la propiedad de que conmutan dos a dos. A continuación, vamos a probar que dos π-bases de Sylow cualesquiera son también conjugadas.

LEMA C.6. *Sea π un conjunto de primos que dividen al orden de un grupo resoluble G. Entonces dos π-bases de Sylow cualesquiera son conjugadas.*

DEMOSTRACIÓN. Sean $(P_1, \ldots, P_r)$ y $(Q_1, \ldots, Q_r)$ dos π-bases de Sylow de G. Por tanto, $P_1 \cdots P_r$ y $Q_1 \cdots Q_r$ son π-subgrupos de Hall de G. Entonces por la Teoría de Hall, existe un elemento $g \in G$ tal que $P_1 \cdots P_r = (Q_1 \cdots Q_r)^g$. Además, $(Q_1 \cdots Q_r)^g = Q_1^g \cdots Q_r^g$. Denotamos por H al subgrupo $Q_1^g \cdots Q_r^g$. Así, $P_1 \cdots P_r = H = Q_1^g \cdots Q_r^g$. Entonces tenemos que $(P_1, \ldots, P_r)$ y $(Q_1^g, \ldots, Q_r^g)$ son bases de Sylow de H. Veamos la razón. Por un lado, como $(P_1, \ldots, P_r)$ es π-base de Sylow de G, también es base de Sylow de H. Por otro lado, como $(Q_1, \ldots, Q_r)$ es π-base de Sylow de G, tenemos que los Q_i conmutan dos a dos, es decir, $Q_iQ_j = Q_jQ_i$ para todo $i, j \in \{1, \ldots, r\}$, con $i \neq j$. Entonces $(Q_iQ_j)^g = (Q_jQ_i)^g$ implica que $Q_i^gQ_j^g = Q_j^gQ_i^g$, es decir, $(Q_1^g, \ldots, Q_r^g)$ es base de Sylow de H. Por tanto, podemos aplicar el resultado general y obtenemos que $(P_1, \ldots, P_r)$ y $(Q_1^g, \ldots, Q_r^g)$ son conjugadas en H. Luego, existe un elemento h de H tal que $P_i^h = Q_i^g$ para todo $i \in \{1, \ldots, r\}$. Por tanto, $P_i = Q_i^{gh^{-1}}$ y así $(P_1, \ldots, P_r)$ y $(Q_1, \ldots, Q_r)$ son conjugadas en G. □

Ahora, probamos el Teorema C.1, el cual reescribimos a continuación.

TEOREMA C.7. *Sea G un grupo tal que sus números de Sylow son coprimos dos a dos. Entonces G cumple que todo conjunto de representantes de Sylow es una base de Sylow.*

DEMOSTRACIÓN. Por el Lema C.3, tenemos que G es resoluble. Sean p y q dos primos diferentes que dividen al orden de G y sea $\pi = \{p, q\}$. Sean P un p-subgrupo de Sylow de G y Q un q-subgrupo de Sylow de G. Si $(\nu_p, \nu_q) = 1$, se tiene que $(|G : N_G(P)|, |G : N_G(Q)|) = 1$. Así obtenemos que $G = N_G(P)N_G(Q)$ y se da la siguiente igualdad:

$$|G : N_G(P) \cap N_G(Q)| = |G : N_G(P)||G : N_G(Q)|.$$

Por otro lado, $\mathcal{H} = \{(P, Q) \mid (P, Q) \ \pi - base\}$ es el conjunto de todas las $\{p, q\}$-bases de G. Como dos π-bases cualesquiera son conjugadas se tiene que

$$|\mathcal{H}| = |G : \mathrm{Stab}_{\mathcal{H}}(P, Q)| = |G : N_G(P) \cap N_G(Q)|.$$

Por tanto, (P, Q) es una π-base de Sylow. Así hemos visto que dados dos primos cualesquiera de G, los subgrupos de Sylow asociados a cada primo conmutan. Por tanto, P_i conmuta con P_j para cualesquiera $p_i \neq p_j$ primos que dividen a $|G|$ y obtenemos el resultado. □

Bibliografía

[1] N. Ahanjideh, A note on the paper entitled "conjugacy classes, characters and products of elements". En preparación.

[2] J. Alperin, R. Lyons, On conjugacy classes of p-elements. *J. Algebra* **19** (1971), 536–537.

[3] A. Beltrán, R. Lyons, A. Moretó, G. Navarro, A. Sáez, P. H. Tiep, Order of products of elements in finite groups. Aceptado en *J. London Math. Soc.*

[4] A. Beltrán, A. Sáez, Existence of normal Hall subgroups by means of orders of products. Aceptado en *Math. Nachr.*

[5] B. Baumslag, J. Wiegold, A sufficient condition for nilpotency in a finite group. arXiv:1411.2877v1.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*. Clarendon Press, Oxford, England, 1985.

[7] E. Bertram, Even permutations as a product of two conjugate cycles. *J. Comb. Theory Ser. A* **12** (1972), 368–380.

[8] M. Conder, Answer to a 1962 question by Zappa on cosets of Sylow subgroups. *Adv. Math.* **313** (2017), 167–195.

[9] J. Cossey, T. Hawkes, On the largest conjugacy class size in a finite group. *Rend. Sem. Mat. Univ. Padova,* **103** (2000), 171–179.

[10] E. C. Dade, M. J. Yadav, Finite groups with product conjugacy classes. *Israel J. Math.* **154** (2008), 29–49.

[11] B. Fein, W.M. Kantor, M. Schacher, Relative Brauer groups, II. *J. Reine Angew. Math.* **328** (1981), 39–57.

[12] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.7.8; 2016, `http://www.gap-system.org.`

[13] D. Goldstein, R. M. Guralnick, Cosets of Sylow p-subgroups and a question of Richard Taylor. *J. Algebra* **398** (2014), 569–573.

[14] R. M. Guralnick, G. Malle, Variations on the Baer–Suzuki theorem. *Math. Z.* **279** (3–4) (2015), 981–1006.

[15] L. Kazarin, A. Martínez-Pastor y M.D. Pérez-Ramos, On the Sylow graph of a group and Sylow normalizers. *Israel J. Math.* **186** (2011), 251-271.

[16] R. M. Guralnick, A. Moretó, Conjugacy classes, characters and products of elements. arXiv:1807.03550v1.

[17] R. M. Guralnick, G. R. Robinson, On extensions of the Baer-Suzuki theorem. *Israel J. Math.* **82** (1–3) (1993), 281–297.

[18] R. M. Guralnick, P. H. Tiep, Lifting in Frattini covers and a characterization of finite solvable groups. *J. Reine Angew. Math.* **708** (2015), 49–72.

[19] P. Hall, Theorems like Sylow's. *Proc. London Math. Soc.* **6** (3) (1956), 286–304.

[20] M. Herzog, G. Kaplan, A. Lev, Representation of permutations as products of two cycles. *Discrete Math.* **285** (2004), 323–327.

[21] B. Huppert, *Endliche Gruppen I.* Springer-Verlag Berlin Heidelberg New York, 1967.

[22] D. H. Husemoller, Ramified coverings of Riemann surfaces. *Duke Math. J.* **29** (1962), 167–174.

[23] I. M. Isaacs, *Character Theory of Finite Groups.* Dover Publications, Inc. New York, 1994.
[24] I. M. Isaacs, *Finite Group Theory.* Amer. Math. Soc. Providence, Rhode Island, 2008.
[25] I. M. Isaacs, Semipermutable π-subgroups. *Arch. Math.* **102** (2014), 1–6.
[26] N. Itô, Note on (LM)-groups of finite order. *Kodai Math. Sem. Rep.* **2** (1-2) (1951), 1–6.
[27] H. Lee, *Triples in Finite Groups and a Conjecture of Guralnick and Tiep*. Ph.D. Thesis, Univ. of Arizona, 2017.
[28] M. L. Lewis, An Overview of graphs associated with character degrees and conjugacy class sizes in finite groups. *Rocky Mountain J. Math.* **38** (1) (2008), 175–211.
[29] X. Liu, Y. Wang, H. Wei, Notes on the length of conjugacy classes of finite groups. *J. Pure and Applied Algebra* **196** (2005), 111–117.
[30] L-C. Kappe, M. Mazur, G. Mendoza, M. B. Ward, On minimal non-p-closed groups and related properties. *Publ. Math. Debrecen* **78** (1) (2011), 219–233.
[31] J. Moori, H. P. Tong-Viet, Products of conjugacy classes simple groups. *Quaestiones Mathematicae* **34** (4) (2011), 433–439.
[32] A. Moretó, Sylow numbers and nilpotent Hall subgroups. *J. Algebra* **379** (2013), 80–84.
[33] A. Moretó, A. Sáez, Prime divisors of orders of products. Aceptado en *Proc. Edim. Math. Soc.*
[34] D. J. S. Robinson, *A course in the theory of groups.* 2nd ed. Springer-Verlag New York, Inc., 1996.
[35] J. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. Reine Angew. Math.* **132** (1907), 85–137.
[36] W. R. Scott, *Group Theory.* Dover Publications, Inc. New York, 1964.
[37] M. Suzuki, Finite groups in which the centralizer of any element of order 2 is 2-closed. *Ann. Math.* **82** (1962), 191–212.
[38] M. Suzuki, *Group Theory II.* Springer-Verlag New York, Inc., 1986.
[39] M. Suzuki, On a class of doubly transitive groups. *Ann. Math., 2nd Series* **75** (1) (1962), 105–145.
[40] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
[41] J. G. Thompson, On a question of L. J. Paige. *Math. Zeitschr.* **99** (1967), 26–27.
[42] H. Wielandt, Zum Satz von Sylow. *Math. Z.* **60** (1954), 407–408.
[43] D. L. Winter, The automorphism group of an extraspecial p-group. *Rocky Mountain J. Math.* **2** (2) (1972), 159–168.
[44] G. Zappa, Un problema sui laterali dei sottogruppi di Sylow di un gruppo finito. *Arch. Math.* **13** (1) (1962), 169–173.
[45] J. Zhang, Sylow numbers of finite groups. *J. Algebra* **176** (1995), 111–123.